IAM

Preguntas frecuentes de IAM

Edición 01

Fecha 2023-07-27

HUAWEI TECHNOLOGIES CO., LTD.

Marcas y permisos


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

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Huawei Technologies Co., Ltd.

Dirección: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Sitio web: https://www.huawei.com

Email: support@huawei.com

Índice

1 Gestión de grupos de usuarios y permisos

1.1 ¿Por qué no están disponibles los permisos para un servicio en la nube?

Síntoma

No se pueden ver los permisos de un servicio en la nube específico cuando se asignan permisos a un grupo de usuarios o a una agencia en la consola de IAM.

Causas posibles

- El servicio no es compatible con IAM. Por lo tanto, no hay permisos disponibles para el servicio en IAM. Para ver los servicios en la nube compatibles con IAM, consulte **Servicios en la nube compatibles**.
- El nombre del servicio o el nombre del permiso son incorrectos.

Soluciones

- **Enviar un ticket de servicio** y solicitar registrar permisos del **servicio relevante** en IAM.
- Compruebe el nombre del servicio en la consola de gestión o en el centro de ayuda y vea los permisos definidos por el sistema proporcionados por el servicio en **Permisos definidos por sistema**.

1.2 ¿Cómo puedo otorgar permisos de servicio en la nube específicos para la región EU-Dublin a los usuarios de IAM?

Síntoma

Ha habilitado servicios en la nube en la región **EU-Dublin** como administrador, y necesita autorizar a los usuarios de IAM en su cuenta para utilizar los servicios en la nube en esta región.

Los usuarios acceden a los servicios en la nube en la región **EU-Dublin** como usuarios virtuales autorizados mediante autenticación federada. No son usuarios reales que existen en el sistema de servicios en la nube, y necesitan estar autorizados en las regiones predeterminadas de Huawei Cloud y la región **EU-Dublin**, respectivamente.

Prerrequisitos

Ha creado un usuario de IAM en una región predeterminada de Huawei Cloud y ha agregado el usuario a un grupo de usuarios. Por ejemplo, ha creado **User-001** de usuarios de IAM y los ha agregado a **UserGroup-001** de grupos de usuarios. Para obtener más información, consulte **Crear un usuario de IAM** y **Agregar usuarios a o quitar usuarios de un grupo de usuarios**.

Procedimiento

Paso 1 Inicie sesión en Huawei Cloud como administrador, haga clic en  en la página de inicio de la consola y seleccione la región **EU-Dublin**.

Paso 2 En la consola de la región **EU-Dublin**, elija **Management & Governance** > **Identity and Access Management**.

Paso 3 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 para crear un grupo con el mismo nombre (**UserGroup-001**).

Paso 4 En la página **User Groups**, haga clic en **Modify** en la fila que contiene el grupo de usuarios creado en **3**.

Paso 5 En el área **Group Permissions**, haga clic en **Attach Policy** en la fila que contiene la región de destino para la autorización de usuario, seleccione los permisos deseados y haga clic en **OK**.

Los permisos asignados a este grupo también se aplicarán a los usuarios de IAM en el grupo de usuarios de Huawei Cloud.

Paso 6 Haga clic en **OK**. La autorización de usuario de IAM para la región **EU-Dublin** está completa.

----Fin

Después de la autorización, inicie sesión en la consola de Huawei Cloud como usuario de IAM, cambie a la región **EU-Dublin**, y use recursos en la nube según lo especificado por los permisos asignados.

1.3 ¿Por qué los permisos otorgados a un usuario no entran en vigor?

Síntoma

Los permisos que concede a un usuario de IAM no han surtido efecto.

Resolución de problemas

1. Los permisos concedidos al grupo de usuarios al que pertenece el usuario son incorrectos.

   Solución: Modifique los permisos concedidos al grupo de usuarios al que pertenece el usuario de IAM como administrador. Para obtener más información, consulte **Modificación de permisos de grupo de usuario** o **Permisos definidos por sistema**.

2. Algunos permisos concedidos al usuario niegan las acciones correspondientes a la operación correspondiente.

   Vea los permisos definidos por el sistema otorgados al usuario de IAM y compruebe si hay una instrucción que deniegue la operación. Para obtener más información, consulte **Sintaxis de política**. Si los permisos definidos por el sistema no pueden cumplir sus requisitos, cree una política personalizada para permitir la operación. Para obtener más información, consulte **Creación de una política personalizada**.

3. El usuario de IAM no se ha agregado al grupo al que el administrador ha asignado permisos.

   Solución: Agregue el usuario al grupo de usuarios de destino como administrador. Para obtener más información, consulte **Adición de usuarios a un grupo de usuario**.

4. Al usuario no se le asignan permisos para un servicio regional en la región correspondiente.

   Asigne permisos para la región relevante al grupo al que pertenece el usuario. Si solo ha asignado al usuario permisos para un proyecto predeterminado específico de región, el usuario no tiene permisos para los subproyectos. En este caso, asigne permisos para el subproyecto requerido. Para obtener más información, consulte **Asignación de permisos a un grupo de usuario**.

5. El usuario de IAM no ha cambiado a la región en la que se ha autorizado al usuario a utilizar recursos en la nube.

   Recuérdele al usuario que cambie a la región donde el usuario está autorizado a usar recursos en la nube. Para obtener más información, consulte **Cambio de regiones**.

6. Si el administrador ha concedido permisos OBS al usuario, los permisos surtirán efecto entre 15 y 30 minutos después de la autorización.

   Compruebe los permisos después de 15 a 30 minutos e inténtelo de nuevo.

7. La caché del navegador no se ha borrado durante mucho tiempo.

   Borre la caché del navegador e inténtelo de nuevo.

8. El servicio (como OBS) proporciona un control de permisos independiente.

   Otorgue los permisos de usuario haciendo referencia a la documentación del servicio. Por ejemplo, consulte **Introducción al control de permiso de OBS**.

9. Si ha concedido permisos a un usuario tanto en IAM como en Enterprise Management, es posible que los permisos para proyectos de empresa no surtan efecto. La autenticación

IAM tiene prioridad sobre la autenticación de Enterprise Management. Si un usuario de IAM tiene el permiso **ECS ReadOnlyAccess** para todos los recursos y el proyecto de empresa A, el usuario puede ver todos los recursos de ECS.

Modifique los permisos del usuario en la consola de IAM.

Preguntas frecuentes relacionadas

Síntoma: Ha concedido a un usuario de IAM solo los permisos necesarios, pero el usuario tiene más permisos.

Causas posibles:

1. Los permisos necesarios otorgados al usuario de IAM tienen permisos de dependencia, que se asignan automáticamente para que los permisos necesarios puedan tener efecto para el usuario.
2. Ha otorgado otros permisos al usuario de IAM en Gestión de proyecto empresarial. Si gestiona proyectos y usuarios mediante IAM, cancele los permisos configurados allí. Para obtener más información, consulte **Eliminación de proyectos empresariales gestionados por un usuario**.

1.4 ¿Cómo puedo conceder a un usuario de IAM permisos para realizar pedidos pero no permitir el pago de pedidos?

Síntoma

Desea conceder a un usuario de IAM permisos para realizar pedidos, pero no permitir que el usuario pague por los pedidos.

Soluciones

Sin embargo, los permisos del sistema del Centro de facturación registrado con IAM no pueden cumplir con sus requisitos. Debe crear una política personalizada que contenga los permisos necesarios y utilizar la política para conceder permisos al usuario de IAM.

Prerrequisitos

Ya ha creado el usuario A y el grupo B de usuarios de IAM y ha agregado el usuario al grupo de usuarios. Para obtener más información, consulte **Creación de un usuario de IAM**.

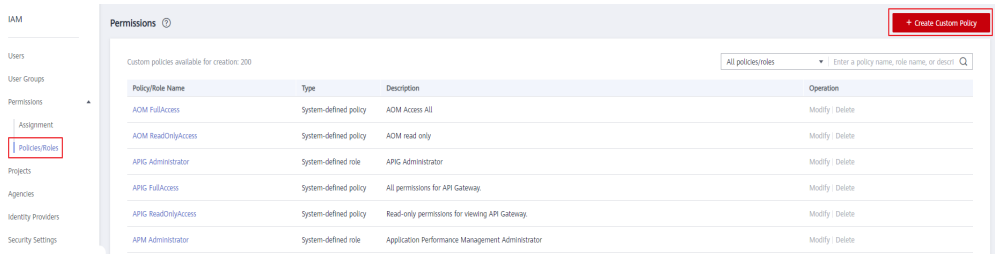
Procedimiento

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

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.

Paso 3 En la consola de IAM, elija **Permissions** > **Policies/Roles** en el panel de navegación y haga clic en **Create Custom Policy** en la esquina superior derecha.

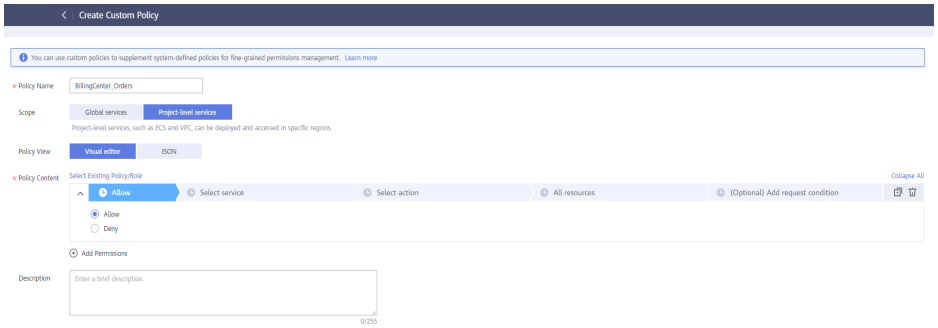
Figura 1-1 Creación de una política personalizada



Paso 4 Establezca el nombre de la política en **BillingCenter_Orders**.

Paso 5 Establezca el ámbito en **Project-level services**.

Figura 1-2 Configuración del ámbito

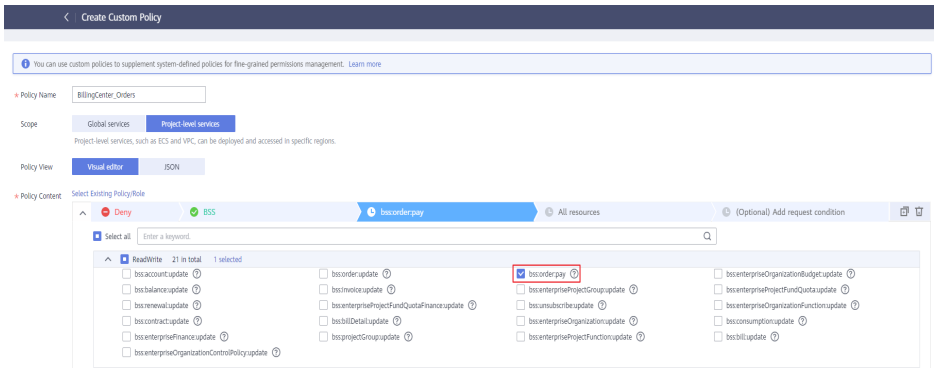


Paso 6 Seleccione **Visual editor**.

Paso 7 En el área **Policy Content**, configure permisos que permitan al usuario realizar pedidos pero que no permitan al usuario pagar los pedidos.

- Configuración de permisos para no permitir el pago de pedidos
  a. Seleccione **Deny**.
  b. Para el servicio en la nube, seleccione **BSS (BSS)**.
  c. En el paso **Select action**, expanda el área **ReadWrite** y seleccione la acción **bss:order:pay**.

  Figura 1-3 Configuración de permisos para no permitir el pago de pedidos



  d. Establezca el tipo de recurso en **All**.

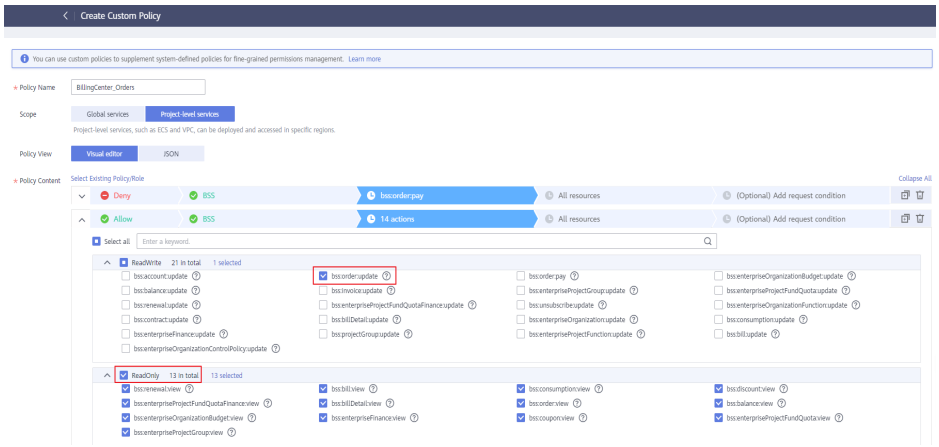
- Configuración de permisos para permitir la colocación de pedidos

a. Seleccione **Allow**.

b. Para el servicio en la nube, seleccione **BSS (BSS)**.

c. En el paso **Select action**, expanda el área **ReadWrite**, seleccione la acción **bss:order:update**, y seleccione todas las acciones en el área **ReadOnly**.

Figura 1-4 Configuración de permisos para permitir la colocación de pedidos



d. Establezca el tipo de recurso en **All**.

Paso 8 Establezca una descripción para la política, por ejemplo, "Permisos para realizar pedidos pero no permitir el pago de pedidos."

Paso 9 Haga clic en **OK**.

Paso 10 Adjunte la política al grupo de usuarios B. 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 adjunta políticas definidas por el sistema. Para obtener más información, consulte **Creación de un grupo de usuario y asignación de permisos**.

Paso 11 Cuando el usuario de IAM inicia sesión y va a la página **My Orders** del Centro de facturación, el botón **Pay** no aparece en la columna **Operation**.

Figura 1-5 La página My Orders se muestra si los permisos se conceden correctamente

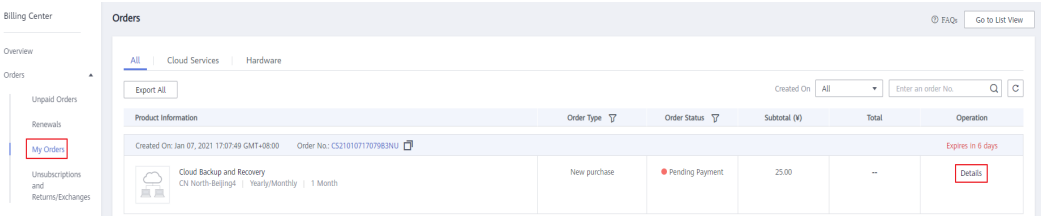
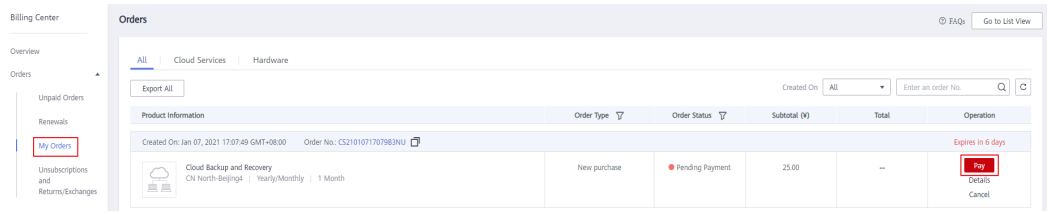


Figura 1-6 Se muestra la página My Orders si no se conceden los permisos



----Fin

2 Gestión de usuarios de IAM

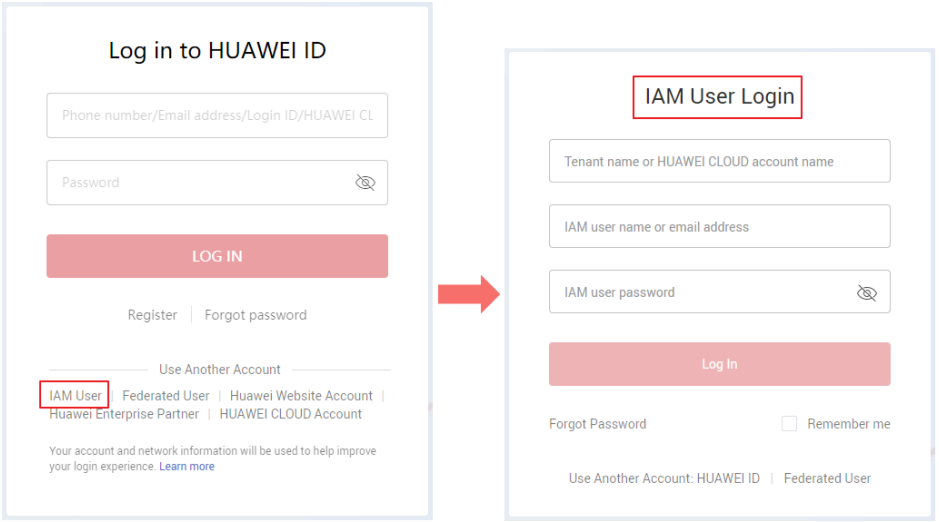
2.1 ¿Por qué falla el inicio de sesión de usuario de IAM?

Síntoma

Un usuario de IAM no puede iniciar sesión y ve un mensaje que indica que el nombre de usuario o contraseña es incorrecto o que el inicio de sesión desde el dispositivo actual no está permitido debido a las reglas de control de acceso establecidas por el administrador.

Resolución de problemas

- **Nombre de usuario o contraseña incorrecta**
  a. Seleccionó una entrada de inicio de sesión incorrecta.
     Haga clic en **IAM User** en la página de inicio de sesión.



  b. Incorrecto nombre de tenant/nombre de cuenta de Huawei Cloud o nombre de usuario de IAM.

Ingrese el correcto nombre de tenant/nombre de cuenta de Huawei Cloud y nombre de usuario de IAM. Si no conoce su nombre de usuario de IAM o el nombre de la cuenta utilizada para crear el usuario de IAM, póngase en contacto con el administrador.

c. Contraseña incorrecta.

Introduzca la contraseña correcta. Si ha olvidado su contraseña, restablezca su contraseña consultando **¿Cómo puedo restablecer mi contraseña?**

d. No ha borrado la caché del navegador después de cambiar o restablecer la contraseña.

Borre la caché del navegador e inicie sesión de nuevo.

- **No se permite iniciar sesión desde el dispositivo actual debido a las reglas de control de acceso establecidas por el administrador.**

a. El administrador ha establecido reglas de control de acceso en la consola IAM para limitar el acceso de Huawei Cloud a intervalos de direcciones IP específicos, bloques CIDR IPv4 o puntos de conexión de VPC.

Solución: Póngase en contacto con el administrador para comprobar las reglas de ACL en la consola e inicie sesión en Huawei Cloud desde un dispositivo permitido, o solicite al administrador que modifique las reglas de ACL. Para obtener más información, consulte **Control de acceso**

2.2 ¿Cómo controlo el acceso de los usuarios de IAM a la consola?

Para garantizar la seguridad de la información del usuario y del sistema, puede configurar una ACL que permita el acceso del usuario solo desde direcciones IP específicas.

Procedimiento

Paso 1 Inicie sesión en la consola de IAM.

Paso 2 En el panel de navegación, elija **Security Settings** > **ACL**.

NOTA

La ACL solo tendrá efecto para los usuarios de IAM que haya creado con su cuenta.

Paso 3 Haga clic en la pestaña **Console Access** y configure las direcciones IP o los bloques CIDR IPv4 a los que se les permite acceder a la consola.

- **IP Address Ranges**: Permitir a los usuarios acceder al sistema mediante direcciones IP en intervalos específicos.
- **IPv4 CIDR Blocks**: Permitir a los usuarios acceder al sistema mediante bloques CIDR IPv4 específicos.

  Por ejemplo: **10.10.10.10/32**.

NOTA

Si especifica **IP Address Ranges** y **IPv4 CIDR Blocks**, los usuarios pueden acceder al sistema si sus direcciones IP cumplen las condiciones especificadas por cualquiera de los dos parámetros.

Paso 4 Haga clic en **Save**.

----Fin

3 Configuraciones de seguridad

3.1 ¿Cómo puedo habilitar la verificación de inicio de sesión?

Para garantizar la seguridad de la cuenta, se recomienda habilitar la verificación de inicio de sesión.

Después de habilitar esta función, usted y los usuarios de IAM creados con su cuenta deben introducir códigos de verificación generados por el dispositivo MFA virtual enlazado, códigos de verificación por SMS o códigos de verificación por correo electrónico en la página **Login Verification** durante el inicio de sesión.

Si desactiva esta función, usted y los usuarios de IAM solo tendrán que introducir el nombre de cuenta/nombre de usuario y contraseña durante el inicio de sesión.

Procedimiento

- Habilitar la verificación de inicio de sesión para un usuario de IAM en la consola de IAM como administrador

Paso 1 En el panel de navegación, elija **Users**.

Paso 2 Haga clic en **Security Settings** en la fila que contiene el usuario de destino.

Paso 3 En la pestaña **Security Settings**, en el área **Login Protection**, seleccione un método de verificación e introduzca un código de verificación.

Paso 4 Haga clic en **OK**.

----Fin

- Habilitar la verificación de inicio de sesión para usted (administrador de cuentas) en la página **Security Settings**

  Realice los siguientes pasos si su cuenta de Huawei Cloud no se ha actualizado a un ID de HUAWEI. Para habilitar la verificación de inicio de sesión para un ID de HUAWEI, vaya al **sitio web de ID de HUAWEI**.

Paso 1 Pase el puntero del ratón sobre el nombre de usuario en la esquina superior derecha y elija **Security Settings** en la lista desplegable.

Paso 2 Haga clic en la pestaña **Critical Operations** y haga clic en **Enable** junto a **Login Protection**.

Paso 3 En la página **Login Protection**, seleccione **Enable**, seleccione un método de verificación e introduzca un código de verificación.

Paso 4 Haga clic en **OK**.

----Fin

Operaciones relacionadas

Puede cambiar el método de verificación de inicio de sesión de sus usuarios o cuenta de IAM:

- Para cambiar el método de verificación de inicio de sesión de un usuario de IAM, vaya a la lista de usuarios en la consola de IAM, haga clic en **Security Settings** en la fila que contiene el usuario, haga clic en  junto a **Verification Method** en **Login Protection** y, a continuación, cambie el método de verificación.
- Para cambiar el método de verificación de inicio de sesión de su cuenta, vaya a la página **Security Settings**. En la pestaña **Critical Operations**, haga clic en **Change** junto a **Login Protection** y, a continuación, cambie el método de verificación.

3.2 ¿Cómo desactivo la verificación de inicio de sesión?

Para garantizar la seguridad de la cuenta, se recomienda habilitar la verificación de inicio de sesión.

Después de habilitar esta función, usted y los usuarios de IAM creados con su cuenta deben introducir códigos de verificación generados por el dispositivo MFA virtual enlazado, códigos de verificación por SMS o códigos de verificación por correo electrónico en la página **Login Verification** durante el inicio de sesión.

Si desactiva esta función, usted y los usuarios de IAM solo tendrán que introducir el nombre de cuenta/nombre de usuario y contraseña durante el inicio de sesión.

Deshabilitar la verificación de inicio de sesión de usuario de IAM como administrador

- Un administrador puede deshabilitar la verificación de inicio de sesión para un usuario de IAM en la consola de IAM de la siguiente manera:

Paso 1 En el panel de navegación, elija **Users**.

Paso 2 Haga clic en **Security Settings** en la fila que contiene el usuario de destino.

Paso 3 En la página de la pestaña **Security Settings**, haga clic en junto a **Verification Method** en **Login Protection** y seleccione **Disabled**.

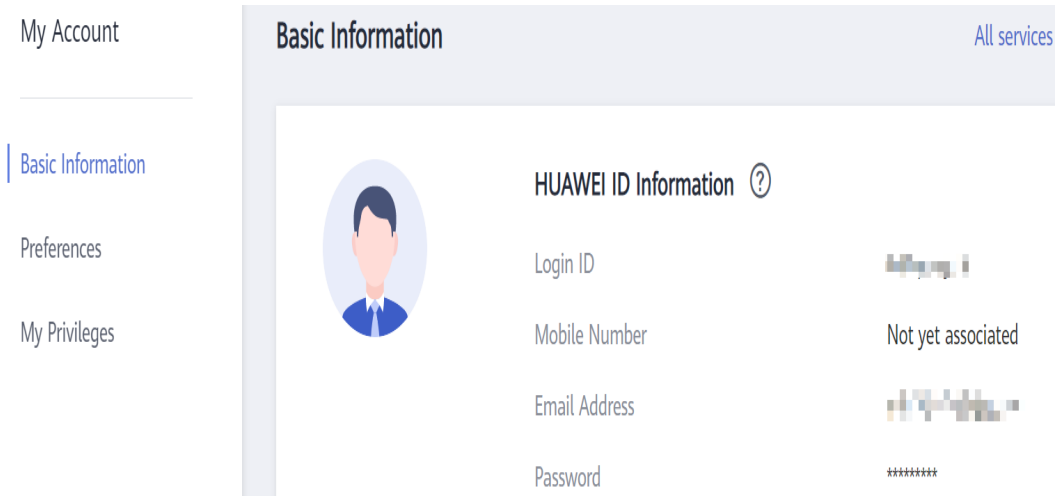
Paso 4 Haga clic en **OK**.

----Fin

Deshabilitar la verificación de inicio de sesión del administrador

Comprueba si la cuenta actual es un ID de HUAWEI o una cuenta de Huawei Cloud haciendo clic en el nombre de la cuenta de inicio de sesión en la esquina superior derecha, eligiendo **My Account** en la lista desplegable, y comprobar si el ID de HUAWEI o Huawei Cloud se muestran en el área **Basic Information**. Si se muestra **HUAWEI ID Information** en el área **Basic Information**, la cuenta actual es un ID de HUAWEI. Si se muestra **Huawei Cloud** en esta área, la cuenta actual es una cuenta de Huawei Cloud. Deshabilitar la verificación de inicio de sesión para un ID de Huawei realizando las operaciones descritas en **Deshabilitar la función de verificación de inicio de sesión para un ID de Huawei**. Deshabilite la verificación de inicio de sesión para una cuenta de Huawei Cloud realizando las operaciones descritas en **Deshabilitar la verificación de inicio de sesión para usted (administrador de cuenta)**.

Figura 3-1 Información del ID de HUAWEI



- Desactivación de la función de verificación de inicio de sesión para un ID de Huawei

Elija **Huawei Account Center** > **Account & Security** > **Security Verification** > **Two-step verification**, haga clic en **Disable**, e introduzca la información de verificación para deshabilitar la protección de inicio de sesión.

- Deshabilitar la verificación de inicio de sesión para usted (administrador de cuentas) en la página **Security Settings**

Paso 1 Pase el puntero del ratón sobre el nombre de usuario en la esquina superior derecha y elija **Security Settings** en la lista desplegable.

Paso 2 Haga clic en la pestaña **Critical Operations** y haga clic en **Change** junto a **Login Protection**.

Paso 3 En la página **Login Protection**, seleccione **Disable**.

Paso 4 Haga clic en **OK**.

----Fin

3.3 ¿Cómo cambio el método de verificación para realizar operaciones críticas?

Síntoma

Si la protección de operaciones está habilitada, los usuarios de su cuenta pueden continuar con una operación crítica, como eliminar un recurso y crear una clave de acceso, solo después de que los usuarios o la persona especificada completen la verificación.

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.

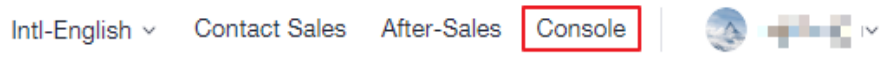
- Para cambiar el método de verificación de **Autoverificación** a **Verificación por otra persona**, consulte **Autoverificación**.
- Para cambiar el método de verificación de **Verificación por otra persona** a **Autoverificación** o para cambiar el número de teléfono móvil o la dirección de correo electrónico para la verificación, consulte **Verificación por otra persona**.

Procedimiento

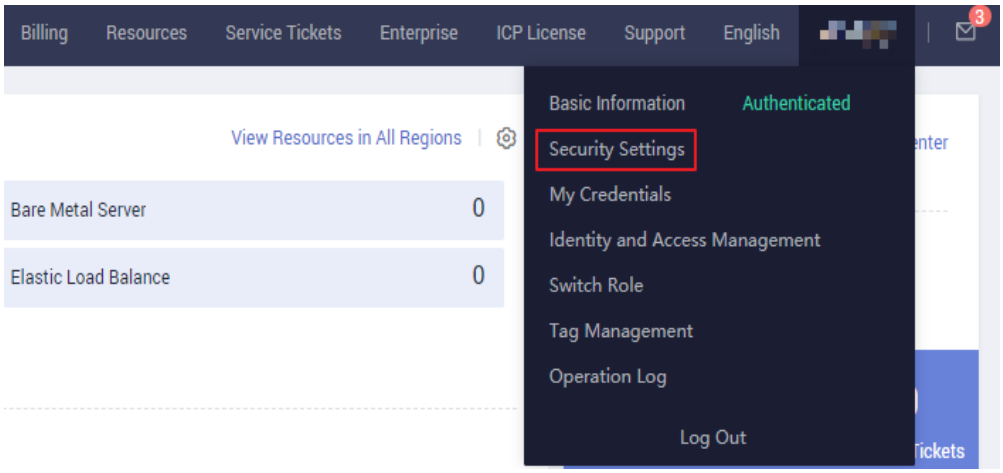
- **El método de verificación actual es la Autoverificación.**

Paso 1 Haga clic en **Console** en la esquina superior derecha.

Figura 3-2 Acceso a la consola de gestión



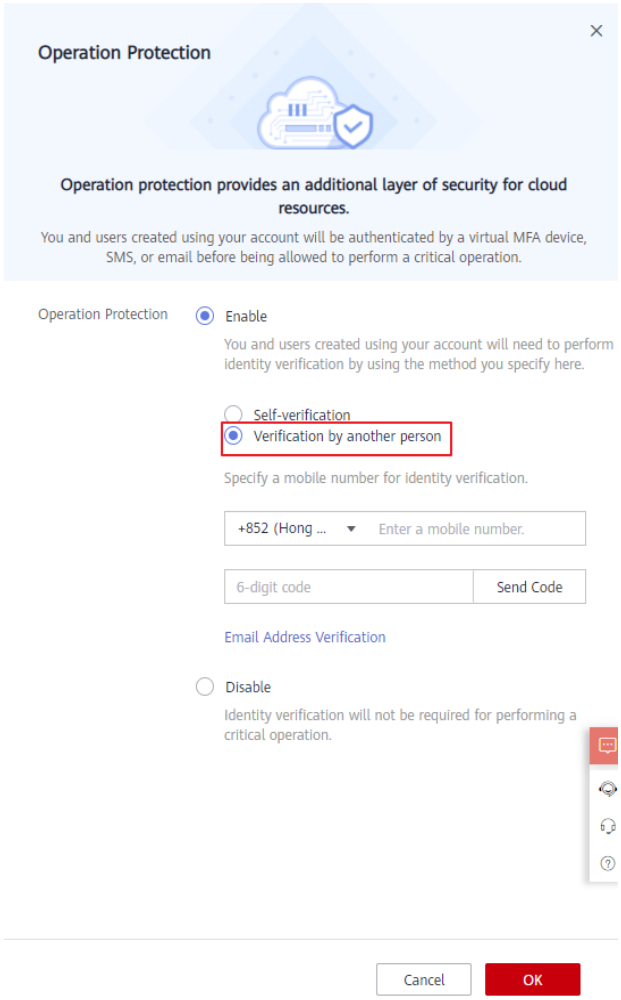
Paso 2 En la consola de gestión, coloque el puntero del ratón sobre el nombre de usuario en la esquina superior derecha y elija **Security Settings** en la lista desplegable.



Paso 3 En la página **Security Settings**, haga clic en la pestaña **Critical Operations** y haga clic en **Change** junto a **Operation Protection**.

Paso 4 En la página **Operation Protection**, seleccione **Verification by another person**, ingrese el número de teléfono móvil o la dirección de correo electrónico para la verificación e ingrese el código de verificación.

Figura 3-3 Configuración de protección de operación



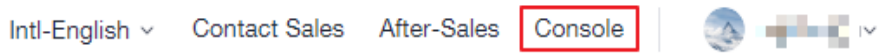
Paso 5 Haga clic en **OK**.

----Fin

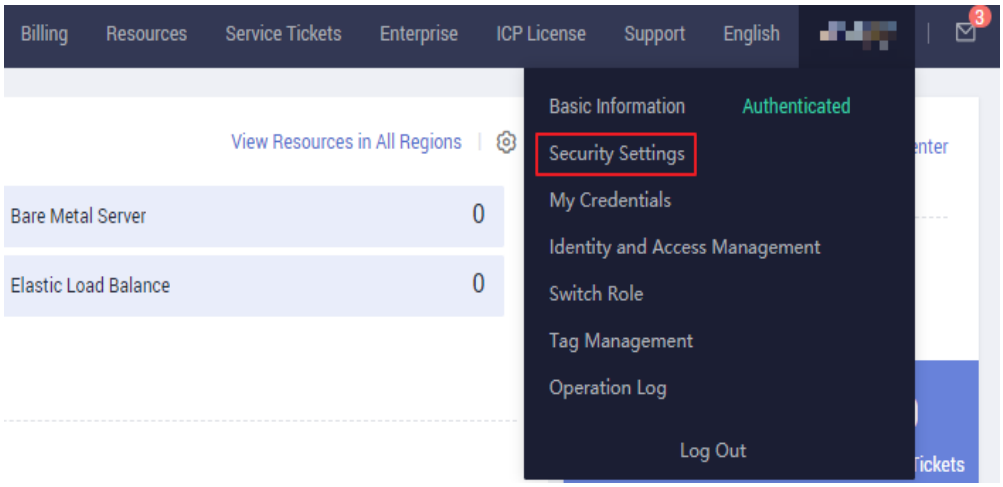
- **El método de verificación actual es Verificación por otra persona.**

Paso 1 Haga clic en **Console** en la esquina superior derecha.

Figura 3-4 Acceso a la consola de gestión



Paso 2 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.



Paso 3 En la página **Security Settings**, haga clic en la pestaña **Critical Operations** y haga clic en **Change** junto a **Operation Protection**.

Paso 4 En la página **Operation Protection**, seleccione **Disable** y haga clic en **OK**. Ingrese el código de verificación y haga clic en **OK**.

Paso 5 En la página de la pestaña **Critical Operations**, haga clic en **Enable** junto a **Operation Protection**.

Paso 6 En la página **Operation Protection**, seleccione **Self-verification** o **Verification by another person**.

Si selecciona **Verification by another person**, complete la verificación para asegurarse de que el método de verificación esté disponible.

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

Paso 7 Haga clic en **OK**.

----Fin

3.4 ¿Cómo desactivo la protección de la operación?

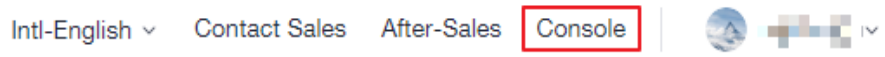
Síntoma

Si la protección de operación está habilitada, los usuarios de su cuenta pueden continuar con una operación crítica (por ejemplo, eliminar un recurso y crear una clave de acceso) solo después de que los usuarios o la persona especificada completen la verificación. Para deshabilitar la protección de operación, realice el siguiente procedimiento.

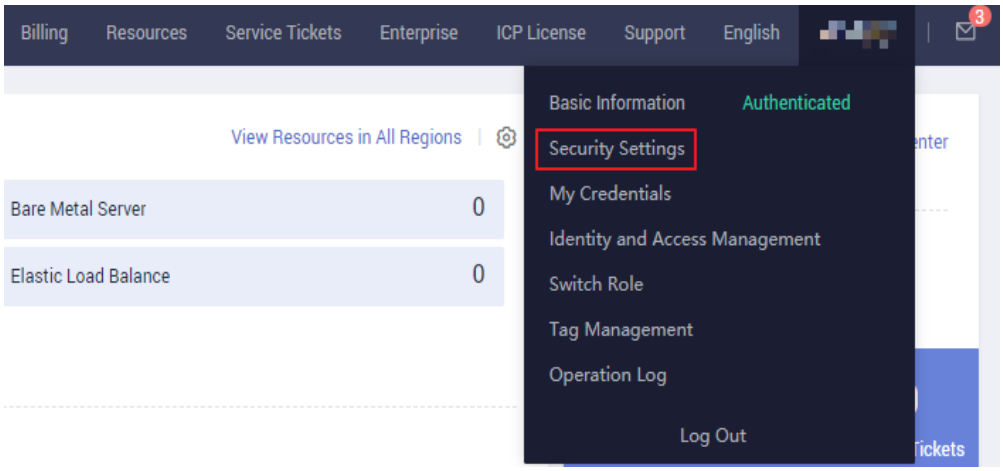
Procedimiento

Paso 1 Haga clic en **Console** en la esquina superior derecha.

Figura 3-5 Acceso a la consola de gestión



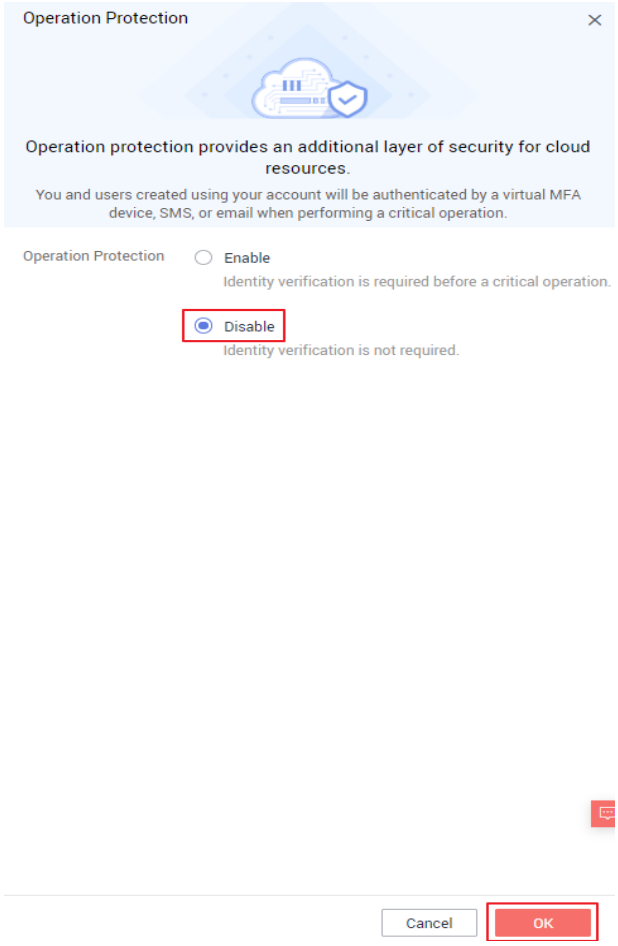
Paso 2 En la consola de gestión, coloque el puntero del ratón sobre el nombre de usuario en la esquina superior derecha y elija **Security Settings** en la lista desplegable.



Paso 3 En la página **Security Settings**, haga clic en la pestaña **Critical Operations** y haga clic en **Change** junto a **Operation Protection**.

Paso 4 Seleccione **Disable** y haga clic en **OK**. Ingrese el código de verificación y haga clic en **OK**.

Figura 3-6 Deshabilitación de la protección de operaciones



----Fin

3.5 ¿Cómo puedo vincular un dispositivo MFA virtual?

La autenticación multifactor (MFA) agrega una capa adicional de protección sobre su nombre de usuario y contraseña. Después de habilitar la verificación de inicio de sesión basada en MFA, debe ingresar los códigos de verificación después de autenticar su nombre de usuario y contraseña. MFA, junto con su nombre de usuario y contraseña, garantiza la seguridad de su cuenta y recursos.

Los dispositivos MFA pueden estar basados en hardware o software. Sin embargo, IAM solo admite dispositivos MFA virtuales.

Un dispositivo MFA virtual es una aplicación que genera códigos de 6 dígitos de acuerdo con el algoritmo de contraseña de un solo uso basada en el tiempo (TOTP). Las aplicaciones MFA pueden ejecutarse en dispositivos móviles (incluidos teléfonos inteligentes) y son fáciles de usar.

Prerrequisitos

Ha instalado una aplicación MFA (por ejemplo, Google Authenticator) en su teléfono móvil.

Procedimiento

- **Cuenta de Huawei Cloud o usuario de IAM**

Paso 1 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.

Paso 2 En la pestaña **Critical Operations**, haga clic en **Bind** junto a **Virtual MFA Device**.

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

- Escanear 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**. A continuación, su cuenta se agrega a la aplicación.

- Introduzca la clave secreta

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

  NOTA

  Para asegurarse de que puede realizar la verificación basada en MFA correctamente, confirme que ha activado la opción de configuración automática de hora en su teléfono móvil.

Paso 4 Vea el código 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 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.

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

Paso 3 En el sitio web de ID de HUAWEI, elija **Account & security** y enlaza un dispositivo MFA virtual en el área **Security verification**.

----Fin

Preguntas Frecuentes Relacionadas

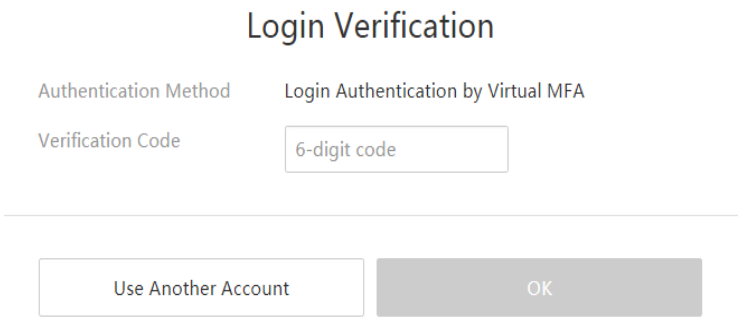
3.6 ¿Cómo obtengo un código de verificación MFA virtual?

3.7 ¿Cómo puedo desvincular o quitar un dispositivo MFA virtual?

3.8 ¿Por qué falla la autenticación de MFA?

3.6 ¿Cómo obtengo un código de verificación MFA virtual?

Si habilita la protección de inicio de sesión virtual basada en MFA o la protección de operación, debe proporcionar códigos de verificación de MFA cuando inicie sesión en la plataforma en la nube o realice una operación crítica. La siguiente figura muestra la página de verificación de inicio de sesión.



Abra la aplicación MFA enlazada y vea los códigos de verificación que se muestran para su cuenta.

NOTA

Si la verificación falla, resuelve el problema haciendo referencia a **3.8 ¿Por qué falla la autenticación de MFA?**

3.7 ¿Cómo puedo desvincular o quitar un dispositivo MFA virtual?

- Si el dispositivo MFA virtual vinculado a su cuenta está disponible, puede desvincular el dispositivo MFA haciendo referencia a **Desvinculación de un dispositivo MFA virtual**.
- Si el dispositivo MFA virtual vinculado a su cuenta no está disponible, no puede desvincular el dispositivo MFA, pero puede eliminarlo haciendo referencia a **Eliminación del dispositivo MFA virtual**.

Los usuarios de IAM pueden enlazar otro dispositivo MFA virtual en la página **Security Settings**. Para más detalles, consulte **3.5 ¿Cómo puedo vincular un dispositivo MFA virtual?**

Desvinculación de un dispositivo MFA virtual

1. Inicie sesión en la consola de gestión.
2. Pase el puntero del ratón sobre el nombre de usuario en la esquina superior derecha y elija **Security Settings** en la lista desplegable.
3. En la pestaña **Critical Operations**, haga clic en **Unbind** junto a **Virtual MFA Device**.

   NOTA

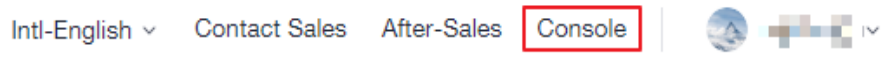
   Si ha actualizado su cuenta de Huawei Cloud a un ID de HUAWEI, será redirigido al sitio web de ID de HUAWEI. Vaya a la página **Account center** > **Account and security**, y haga clic en **Disassociate** junto a **Authenticator** en el área de **Security verification**.
4. Introduzca los códigos de verificación generados por la aplicación MFA.
5. Haga clic en **OK**.

Eliminación del dispositivo MFA virtual

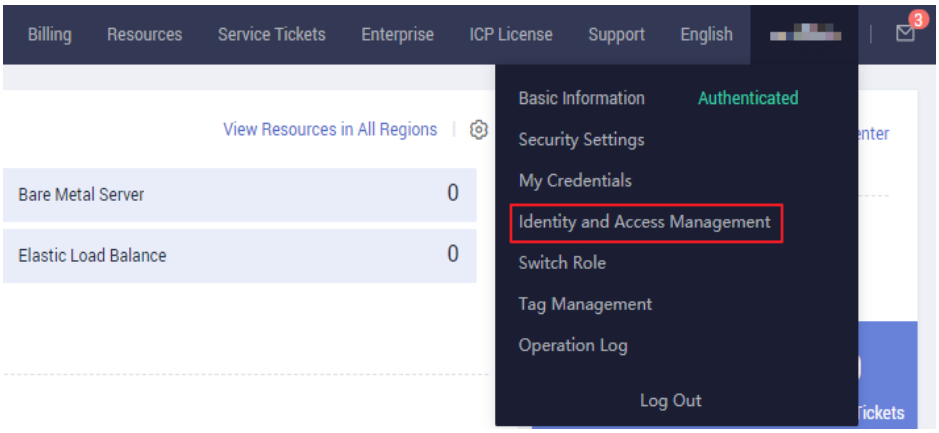
- **Cuenta de Huawei Cloud** o ID de HUAWEI: Si su teléfono móvil no está disponible o el dispositivo MFA virtual vinculado se ha eliminado de su teléfono, **enviar un ticket de servicio** seleccionando **Identity and Access Management** > **Account Security Settings** para quitar el dispositivo MFA virtual de su cuenta, o llame al +86 4000-955-988 para ponerse en contacto con el servicio de atención al cliente.
- **Usuario de IAM**: Si su teléfono móvil no está disponible o el dispositivo MFA virtual vinculado se ha eliminado del teléfono, solicite al **administrador** que quite el dispositivo MFA virtual. El procedimiento para eliminar un dispositivo MFA virtual es el siguiente:

1. Haga clic en **Console** en la esquina superior derecha.

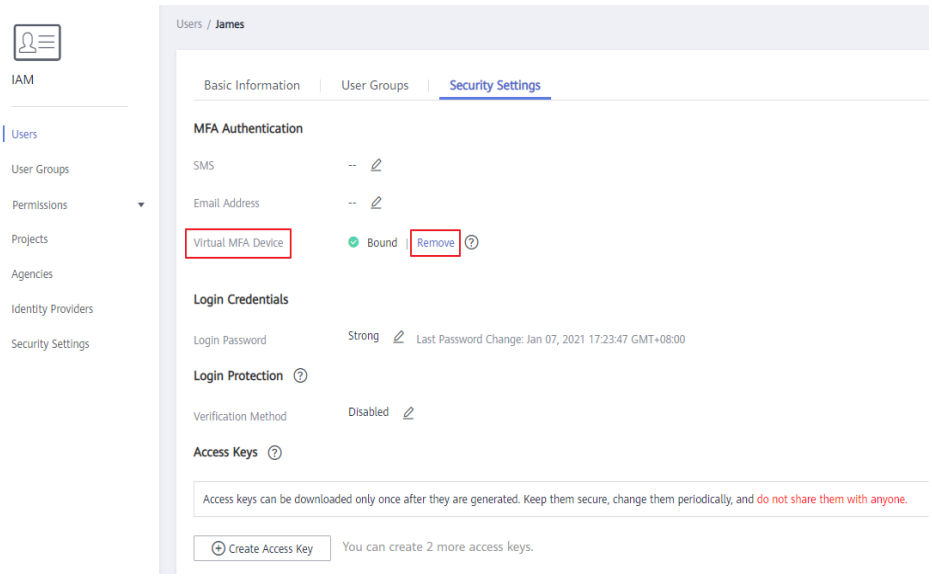
   Figura 3-7 Acceso a la consola de gestión

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.

3. Inicie sesión en la consola de IAM.
4. En la página **Users**, haga clic en **Security Settings** a la derecha del usuario de destino.
5. En la página de la pestaña **Security Settings**, haga clic en **Remove** junto a **Virtual MFA Device**.



6. Haga clic en **Yes**.

3.8 ¿Por qué falla la autenticación de MFA?

Síntoma

La autenticación MFA falla al iniciar sesión o realizar una operación crítica, o vincular o desvincular un dispositivo MFA virtual.

Causas posibles

- Los códigos de verificación son incorrectos.
- Los códigos de verificación han caducado.
- Los códigos de verificación pertenecen a otra cuenta.
- Cuando enlazó de nuevo un dispositivo MFA virtual después de desvincular el anterior, no agregó su cuenta al dispositivo MFA.
- La generación de códigos de verificación MFA está sujeta a ese tiempo. Si la diferencia de tiempo entre su teléfono móvil y el dispositivo MFA virtual es superior a 30 segundos, los códigos de verificación MFA generados en su teléfono móvil fallarán la verificación.

Soluciones

- Introduzca los códigos de verificación correctos.
- Los códigos de verificación se actualizan automáticamente cada 30 segundos. Introduzca dos códigos de verificación consecutivos.
- Asegúrese de que el nombre de cuenta que aparece encima del código de verificación en el autenticador sea el mismo que el nombre de la cuenta utilizada para solicitar la autenticación MFA.
- Para volver a vincular un dispositivo MFA virtual, elimine la información de su cuenta en el dispositivo MFA y, a continuación, agregue su cuenta a él.

- Asegúrese de que la hora en su teléfono móvil es la misma que la hora en el dispositivo MFA virtual e inténtelo de nuevo. (No es necesario considerar la zona horaria en su teléfono móvil, ya que la autenticación MFA se basará en la hora UTC.)

3.9 ¿Por qué no obtengo el código de verificación?

Cuando vincula o cambia el número de teléfono móvil o la dirección de correo electrónico o restablece la contraseña, debe obtener un código de verificación para la autenticación. Si no puede obtener el código, realice las operaciones descritas en esta sección.

¿Por qué no recibo el código de verificación de SMS?

- Compruebe si el número de móvil que ha introducido es correcto. Si no es correcto, ingrese el número de móvil correcto e inténtelo de nuevo.
- Compruebe si su servicio móvil ha sido suspendido debido a atrasos. Si se ha suspendido, despeje el importe pendiente e inténtelo de nuevo una vez que se haya reanudado el servicio móvil. También puede cambiar el número de teléfono móvil asociado a su cuenta.
- Compruebe si el SMS que contiene el código de verificación se ha filtrado o bloqueado como un mensaje no deseado. Si esto ocurre, desactive la función de filtrado o bloqueo de mensajes de SMS.

  NOTA

  Comprueba si hay mensajes que contengan un código de verificación enviado por Huawei Cloud en mensajes basura o spam.

- En algunos escenarios, es posible que los mensajes SMS no se entreguen debido a problemas de red. En este caso, envíe un código de verificación de nuevo o inténtelo de nuevo más tarde. Alternativamente, instale la tarjeta SIM en otro teléfono e inténtelo de nuevo.

Si el error persiste después de realizar las operaciones anteriores, pruebe la verificación MFA virtual o por correo electrónico.

Si tanto su teléfono móvil como su dirección de correo electrónico no pueden recibir el código de verificación, póngase en contacto con el servicio de atención al cliente.

¿Por qué no recibo el código de verificación de correo electrónico?

- Verifique si la dirección de correo ingresada es correcta. Si no es correcto, ingrese la dirección de correo electrónico correcta e inténtelo de nuevo.
- Compruebe si su buzón es normal y verifique la carpeta de correo no deseado.
- Agregue las siguientes direcciones de correo electrónico a la lista blanca: **noreplyhk01@mail01.huawei.com** y **noreplydl01@mail01.huawei.com**.
- Es posible que los correos no se entreguen debido a problemas de red. En este caso, envíe un código de verificación de nuevo o inténtelo de nuevo más tarde.

Si el error persiste después de realizar las operaciones anteriores, pruebe la verificación por SMS o MFA virtual.

Si tanto su teléfono móvil como su dirección de correo electrónico no pueden recibir el código de verificación, póngase en contacto con el servicio de atención al cliente.

3.10 ¿Por qué mi cuenta está bloqueada?

Síntoma

- Cuando inicia sesión en el sistema, aparece un mensaje que indica que su cuenta está bloqueada y que puede usarse para volver a iniciar sesión después de 15 minutos.
- Cuando se invoca a una API (como la API utilizada para **obtener un token de usuario**) cuyos parámetros de solicitud incluyen una contraseña, se muestra la siguiente respuesta:

```
{
    "error": {
        "code": 401,
        "message": "The account is locked.",
        "title": "Unauthorized"
    }
}
```

Causas posibles

Su cuenta está bloqueada durante 15 minutos debido a excepciones de seguridad, por ejemplo, ha introducido contraseñas incorrectas varias veces, o la cuenta se ha utilizado con frecuencia para iniciar sesión desde diferentes ubicaciones.

Soluciones

- Si su cuenta está bloqueada debido a operaciones incorrectas, espere 15 minutos e inténtelo de nuevo. No inicie sesión ni introduzca la contraseña dentro de este período.
- Si ha olvidado su contraseña de inicio de sesión, restablezca su contraseña. Para más detalles, consulte **4.1 ¿Cómo puedo restablecer mi contraseña?**
- Si la cuenta está bloqueada sin motivo alguno, cambie la contraseña. Para más detalles, consulte **4.2 ¿Cómo cambio mi contraseña?**

3.11 ¿Por qué mi política de control de acceso no entra en vigor?

Síntoma

Ha establecido una política de control de acceso a la API, pero los usuarios de IAM que no cumplan con los requisitos de la política aún pueden acceder a Huawei Cloud mediante API.

Soluciones

1. La política de control de acceso de API aún no ha entrado en vigor.

   Las políticas de control de acceso de API entran en vigor dentro de **2 hours** una vez establecidas.

2. El control de acceso a la API no se admite en su región actual.

   Actualmente, el control de acceso de API solo se admite en las regiones **CN Southwest-Guiyang1**, **CN South-Shenzhen** y **CN East-Shanghai1**.

3. El control de acceso a la API no tiene efecto para OBS.

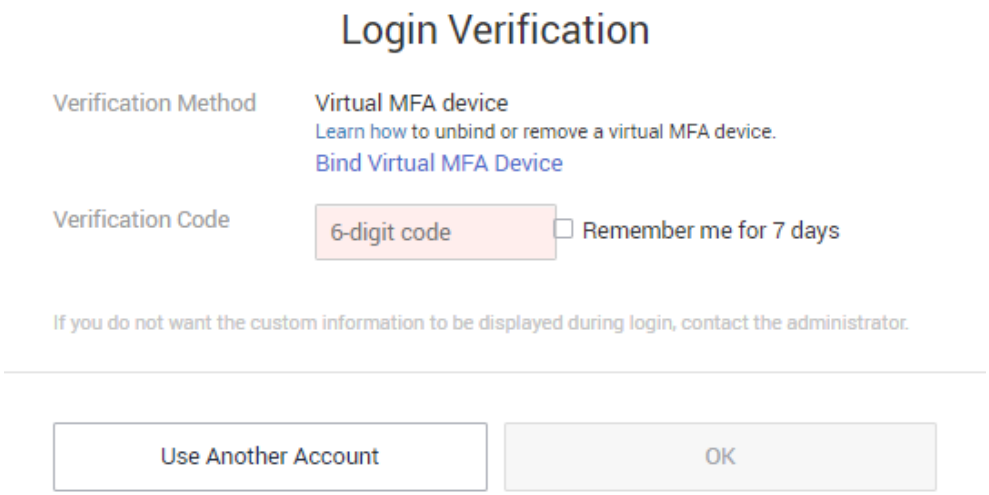
OBS no es compatible con las políticas de control de acceso de API. Para restringir el acceso a los recursos de OBS, consulte **Restricción del acceso al bucket a direcciones IP específicas**.

Si no se aplica ninguno de los escenarios anteriores, modifique la política de control de acceso de la API. Si la política aún no entra en vigor, **envíe un ticket de servicio** seleccionando **Identity and Access Management** > **Account Security Settings** y especificando "control de acceso a API", o llámenos al +86 4000-955-988.

3.12 ¿Por qué todavía necesito realizar MFA durante el inicio de sesión después de desvincular el dispositivo MFA virtual?

Síntoma

Ha desvinculado o eliminado el dispositivo MFA virtual, pero aún debe verificar su identidad a través de MFA al iniciar sesión en Huawei Cloud.



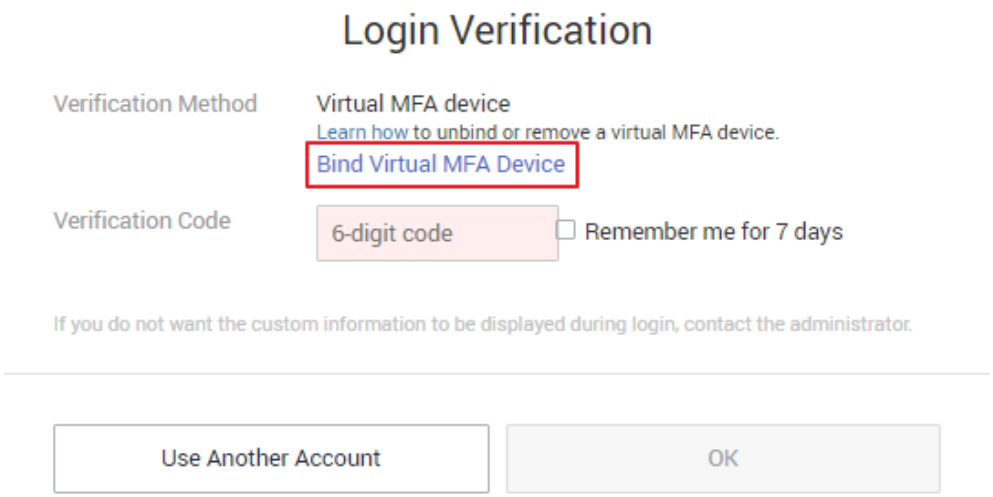
Causas posibles

Aunque el dispositivo MFA virtual se ha desvinculado o eliminado, la protección de inicio de sesión sigue estando habilitada. Por lo tanto, todavía se requiere la verificación de inicio de sesión.

Soluciones

- Cuando inicie sesión en Huawei Cloud, vuelva a vincular un dispositivo MFA virtual y utilícelo para verificar su identidad.

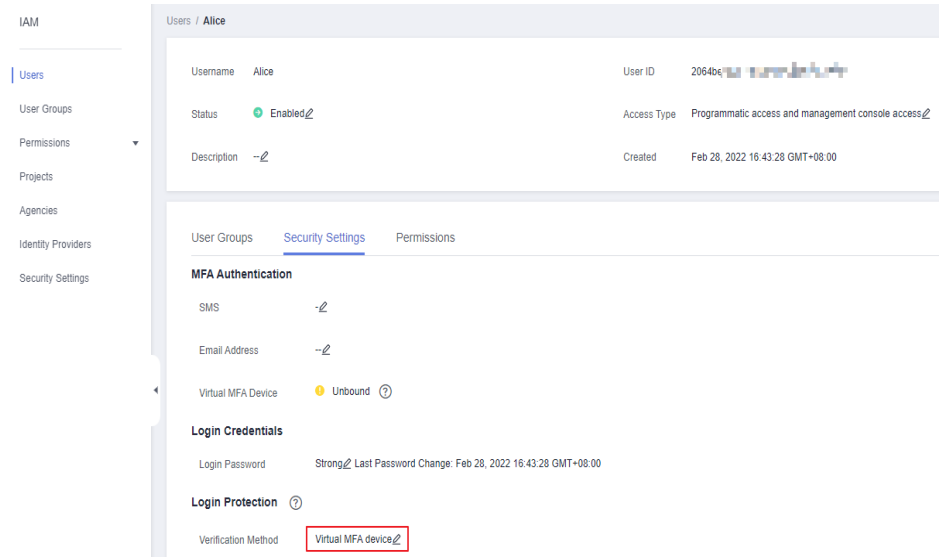
  Haga clic en **Bind Virtual MFA Device** en el cuadro de diálogo **Login Verification**. Para obtener más información, consulte **3.5 ¿Cómo puedo vincular un dispositivo MFA virtual?**.



- Si es usuario de IAM, solicite al administrador que cambie el modo de verificación de inicio de sesión a número de teléfono móvil o dirección de correo electrónico y vuelva a iniciar sesión.

  Si es administrador, inicie sesión en la consola de IAM, haga clic en el nombre de usuario para ir a la página de detalles del usuario y cambie el modo de verificación de inicio de sesión en la página de fichas **Security Settings**.

Figura 3-8 Autenticación de MFA virtual



4 Contraseñas y credenciales

4.1 ¿Cómo puedo restablecer mi contraseña?

Si ha olvidado la contraseña de su usuario o cuenta de IAM, restablezca la contraseña consultando **Restablecer la contraseña de usuario de IAM o la contraseña de la cuenta de Huawei Cloud**.

Si ha olvidado la contraseña de su ID de HUAWEI, restablezca la contraseña consultando **Restablecimiento de la contraseña de ID de HUAWEI**.

NOTA

En esta sección solo se describe cómo recuperar la contraseña de un usuario de IAM, una cuenta de Huawei Cloud o un ID de HUAWEI.

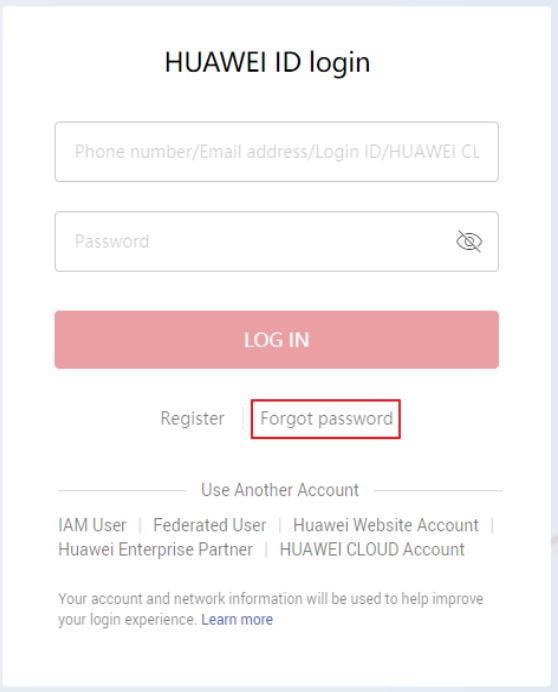
Si aparece un mensaje de error que indica que la cuenta no es válida o no es compatible durante la recuperación de contraseñas, esto significa que la cuenta no es un usuario de IAM, una cuenta de Huawei Cloud o un ID de HUAWEI. Compruebe si el nombre de cuenta introducido es correcto. Si no tiene un 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**.

Restablecer la contraseña de usuario de IAM o la contraseña de la cuenta de Huawei Cloud

Si usted es un usuario de IAM y no ha vinculado ninguna dirección de correo electrónico o número de móvil a su cuenta, solicite al administrador que **restablezca su contraseña**.

Paso 1 En la página de inicio de sesión de Huawei Cloud, haga clic en **Forgot password**.

Figura 4-1 Restablecer la contraseña de usuario de IAM o la contraseña de la cuenta de Huawei Cloud



Paso 2 Haga clic en **Reset Huawei Cloud account password**.

Paso 3 Especifique la cuenta o el usuario de IAM para el que desea restablecer la contraseña e introduzca el código CAPTCHA.

NOTA

- Cuenta: Creada tras registrarse correctamente en Huawei Cloud. La cuenta tiene permisos de acceso completos para todos sus servicios y recursos en la nube y realiza pagos por el uso de estos recursos. Después de iniciar sesión en la cuenta, verá la cuenta marcada como **Enterprise administrator** en la página **Users**.
- Usuario de IAM: Creado con su cuenta. Los usuarios de IAM pueden iniciar sesión en Huawei Cloud con el nombre de cuenta, el nombre de usuario y la contraseña, y luego usar recursos basados en los permisos asignados. Los usuarios de IAM no poseen recursos y no pueden realizar pagos.
- Si usted es un usuario de IAM y no ha vinculado una dirección de correo electrónico o número de teléfono móvil a su cuenta, solicite al administrador que restablezca su contraseña. Para obtener más información, consulte **Cambio de la contraseña de inicio de sesión de un usuario de IAM**.

Paso 4 Seleccione nombre de cuenta/dirección de correo electrónico o verificación del número de móvil, introduzca la información de verificación según se le solicite y haga clic en **Next**.

NOTA

- Asegúrese de que el número de teléfono móvil o la dirección de correo electrónico que ingresó sea correcta. De lo contrario, la contraseña no se puede restablecer.
- Si no recibe el código de verificación, consulte **3.9 ¿Por qué no obtengo el código de verificación?**.

Paso 5 Ingrese una nueva contraseña, introdúzcala de nuevo y haga clic en **Next**.

Paso 6 Haga clic en **Log In** para iniciar sesión con la nueva contraseña.

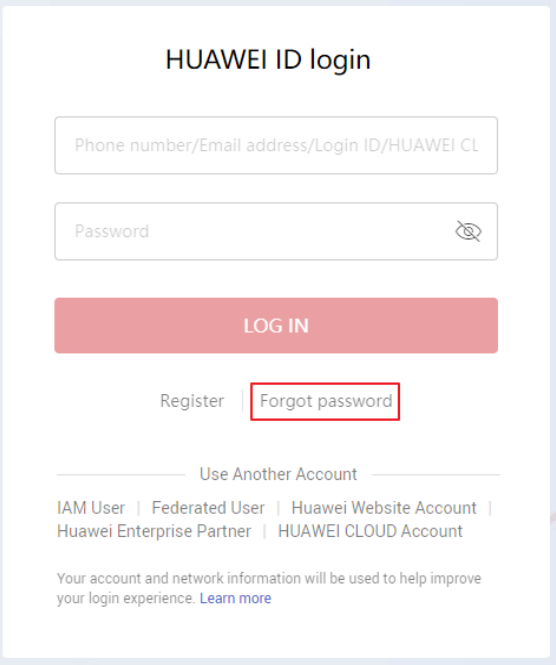
----Fin

Restablecimiento de la contraseña de ID de HUAWEI

- Si no puede restablecer la contraseña de su ID de HUAWEI porque el número de teléfono móvil o la dirección de correo electrónico asociada con el ID de HUAWEI no está disponible, cambie el número de teléfono móvil o la dirección de correo electrónico en el **sitio web de ID de HUAWEI**, e inténtelo de nuevo.
- Si el número de teléfono móvil o la dirección de correo electrónico asociada a su ID de HUAWEI sigue disponible:

Paso 1 En la página de inicio de sesión de Huawei Cloud, haga clic en **Forgot password**.

Figura 4-2 Restablecimiento de la contraseña del ID de HUAWEI



Paso 2 Haga clic en **Regain access to your HUAWEI ID**.

Paso 3 Ingrese su ID de inicio de sesión o el número de teléfono móvil/dirección de correo electrónico utilizada para registrar su ID de HUAWEI y haga clic en **Next**.

Paso 4 (Opcional) Si ingresaste su ID de inicio de sesión en **3**, vaya a **5**. Si ha introducido un número de teléfono móvil o una dirección de correo electrónico en **3**, seleccione el ID de HUAWEI para el que desea restablecer la contraseña.

Paso 5 Realice la verificación y haga clic en **Next**.

NOTA

Si no recibe el código de verificación, consulte **3.9 ¿Por qué no obtengo el código de verificación?**.

Paso 6 Ingrese una nueva contraseña, introdúzcala de nuevo y haga clic en **OK**.

Paso 7 Elija si desea cerrar sesión en cualquier otro dispositivo o sitio web que use su ID de HUAWEI.

Paso 8 (Opcional) Vincule un dispositivo MFA virtual a su ID de HUAWEI. Para obtener más información, consulte **Autenticación de MFA y dispositivo MFA virtual**.

Paso 9 Haga clic en **RETURN NOW** e **inicie sesión en Huawei Cloud**.

----Fin

4.2 ¿Cómo cambio mi contraseña?

- Si recuerda su contraseña y desea cambiarla, haga lo siguiente:
  - **Cuenta de Huawei Cloud**: Cambiar la contraseña en la página **Basic Information** de My Account.
  - **HUAWEI ID**: Cambiar la contraseña en el centro de cuentas de HUAWEI. Para ello, vaya a la página **Basic Information** de My Account y haga clic en **Manage** junto a **HUAWEI ID Information**. Se le redirige automáticamente a la página **Account & security** del Centro de cuentas de HUAWEI. Restablecer la contraseña en el área **Security center**.
  - **IAM user**: Sitúe el puntero del ratón sobre el nombre de usuario en la esquina superior derecha de la consola y elija **Security Settings**. A continuación, cambie la contraseña en la pestaña **Basic Information**.
- Si ha olvidado su contraseña:
  - Restablecer su contraseña siguiendo las instrucciones en **4.1 ¿Cómo puedo restablecer mi contraseña?**
  - Si usted es un usuario de IAM y no ha vinculado ninguna dirección de correo electrónico o número de teléfono móvil a su cuenta, **solicite al administrador que restablezca su contraseña**.

4.3 ¿Cómo obtengo una clave de acceso (AK/SK)?

- Si tiene una contraseña para iniciar sesión en la consola de gestión, inicie sesión en la consola, mueva el puntero al nombre de usuario en la esquina superior derecha y seleccione **My Credentials** en la lista desplegable. Elija **Access Keys** en el panel de navegación izquierdo y puede ver el ID de clave de acceso (AK) en la lista de claves de acceso. Puede obtener la clave de acceso secreta (SK) del archivo descargado .csv. Para obtener más información, consulte **Claves de acceso**.
- Si no utiliza una contraseña para iniciar sesión en la consola de gestión, solicite al administrador que cree una clave de acceso para usted en la consola de IAM. Para obtener más información, consulte **Gestión de claves de acceso para un usuario de IAM**.

4.4 ¿Qué debo hacer si he olvidado mi clave de acceso (AK/SK)?

Si ha olvidado su clave de acceso, puede eliminarla y crear una nueva. Para obtener más información, consulte **Claves de acceso**.

NOTA

Si es usuario de IAM, mueva el puntero al nombre de la cuenta en la esquina superior derecha de la consola de gestión, elija **Security Settings**, haga clic en la pestaña **Critical Operations** y compruebe el estado de habilitación de la función **Access Key Management**.

- Deshabilitado: Todos los usuarios de IAM bajo la cuenta pueden gestionar (crear, habilitar, deshabilitar y eliminar) sus propias claves de acceso.
- Habilitado: solo los usuarios de IAM a los que se les han concedido los permisos necesarios pueden gestionar las claves de acceso.

Si no puede gestionar sus claves de acceso:

- solicitar al **administrador** que gestione sus claves de acceso. Para obtener más información, consulte **Gestión de claves de acceso para un usuario de IAM**.
- solicite al **administrador** que le asigne los permisos necesarios o deshabilite la gestión de claves de acceso. Para obtener más información, consulte **Asignación de permisos a un usuario de IAM** o **Gestión de clave de acceso**.

4.5 ¿Qué son las credenciales de seguridad temporal (AK/SK y SecurityToken)?

Credenciales de seguridad temporal

Las credenciales de seguridad temporales incluyen claves de acceso temporales (AK/SK) y securityTokens. Solo tienen **temporary access permissions** y son ligeramente diferentes de las credenciales de seguridad permanentes.

Diferencias entre credenciales de seguridad temporales y permanentes

En la siguiente tabla se muestran las diferencias entre los dos tipos de credenciales de seguridad.

Tabla 4-1 Diferencias de credenciales

Concepto	Credenciales Temporales	Credenciales Permanentes
Período de validez	15 minutos a 24 horas	Validez ilimitada
Número de credenciales	Ilimitado	2 credenciales para cada usuario de IAM
Método de obtención	Invocar a la API utilizada para **obtener una clave de acceso temporal**.	Crear una clave de acceso en la página **My Credentials**.
Uso	No se puede incrustar en aplicaciones ni almacenar para su uso posterior, y debe obtenerse de nuevo después de la expiración.	N/A

Ventajas de las credenciales de seguridad temporal

Las credenciales de seguridad temporales son útiles para conceder a los usuarios federados solo los permisos necesarios con un período de validez específico.

Uso de credenciales temporales de seguridad

Se debe usar una clave de acceso junto con un securityToken. Cuando utilice credenciales de seguridad temporales para la autenticación, agregue el campo **x-security-token** al encabezado de solicitud. Para obtener más información, consulte **Guía de firma de solicitud de API**.

4.6 ¿Cómo obtengo un token con permisos de administrador de seguridad?

Un token es una credencial de acceso emitida a un usuario de IAM para llevar su identidad y permisos. Al invocar a las API de IAM u otros servicios en la nube, puede usar esta API para obtener un token de usuario para la autenticación.

Los permisos de un token son determinados por los permisos del usuario que obtiene el token. Solo los usuarios a los que se les ha asignado el rol **Security Administrator** pueden obtener un token con permisos de **Security Administrator**.

Métodos

- Administrador de cuentas: cree un usuario de IAM, asigne el rol **Security Administrator** al usuario y, a continuación, invoque a la API utilizada para **obtener un token de usuario**. El token obtenido tiene los permisos **Security Administrator**.
- Usuario de IAM: Solicite al administrador que le asigne el rol **Security Administrator** y, a continuación, obtenga un token.

Permisos de administrador de seguridad

Tabla 4-2 Permisos de administrador de seguridad

Nombre de permiso	Alcance	Descripción
Security Administrator	Global	Permisos de administrador para IAM, incluidos, entre otros, los siguientes permisos: ● Creación, modificación y eliminación de usuarios de IAM ● Crear, modificar y eliminar grupos de usuarios y concederles permisos ● Creación, modificación y eliminación de políticas personalizadas ● Creación y modificación de proyectos ● Creación, modificación y eliminación de agencias ● Creación, modificación y eliminación de proveedores de identidad ● Configuración de la configuración de seguridad de la cuenta

4.7 ¿Cómo obtengo una clave de acceso (AK/SK) en la región EU-Dublin?

Síntoma

Ha habilitado servicios en la nube en la región **EU-Dublin** como administrador. Usted y los usuarios de IAM en su cuenta deben usar claves de acceso en esta región para la encriptación y la firma.

Los usuarios acceden a los servicios en la nube en la región **EU-Dublin** como usuarios virtuales autorizados mediante autenticación federada. No son usuarios reales que existen en el sistema de servicios en la nube, y necesitan obtener una clave de acceso en las regiones predeterminadas de Huawei Cloud y la región **EU-Dublin**, respectivamente.

El siguiente procedimiento le guiará a través de la creación de una clave de acceso permanente para usted como administrador o para sus usuarios de IAM. Tanto usted como sus usuarios de IAM pueden crear claves de acceso temporales en la página **My Credentials**.

Procedimiento

Paso 1 Cree un usuario de IAM en la región **EU-Dublin** como administrador. Para crear una clave de acceso, vaya a **Paso 2**.

1. Inicie sesión en Huawei Cloud como administrador, haga clic en  en la página de inicio de la consola y seleccione la región **EU-Dublin**.
2. En la consola de la región **EU-Dublin**, elija **Management & Governance** > **Identity and Access Management**.

3. En el panel de navegación de la consola de IAM, elija **Users**.
4. Haga clic en **Create User** en la esquina superior derecha.
5. En la página **Create User**, establezca la información del usuario. Para obtener más información, consulte **Creación de un usuario de IAM**.

   Para identificar la entidad que utiliza una clave de acceso, cree un usuario IAM con el mismo nombre que el usuario IAM correspondiente o su cuenta.
6. Haga clic en **OK**.

Paso 2 Obtenga una clave de acceso para el usuario de IAM.

1. Inicie sesión en la consola de IAM en la región **EU-Dublin** como administrador.
2. En la página **Users** de la consola de IAM, haga clic en **Security Settings** en la columna **Operation** de la fila que contiene el usuario de IAM creado en **1**.
3. En la página de pestaña de **Security Settings** de la página de detalles del usuario de IAM, haga clic en **Create Access Key**.
4. (Opcional) Introduzca una descripción para la clave de acceso.
5. Haga clic en **OK**. Se crea la clave de acceso.
6. Descargue el archivo de clave de acceso.

   NOTA

   - Cada usuario puede tener un máximo de dos claves de acceso con validez ilimitada. Para garantizar la seguridad de la cuenta, guárdelas correctamente.
   - Usted y el usuario de IAM pueden usar la clave de acceso solo en la región **EU-Dublin**.
7. (Opcional) Proporcione la clave de acceso al usuario de IAM.

----Fin

5 Gestión de proyectos

5.1 ¿Cuáles son las diferencias entre IAM y Enterprise Management?

Enterprise Management permite a las empresas gestionar recursos en la nube por nivel de proyecto y organización. Incluye proyectos empresariales, contabilidad, aplicaciones, y gestión de personal. IAM es un servicio de gestión de identidad que proporciona autenticación de identidad, gestión de permisos y control de acceso.

Puede usar IAM y Enterprise Management para gestionar usuarios y permisos de acceso. Enterprise Management también permite la gestión de aplicaciones y contabilidad, y admite una autorización más detallada para el uso de recursos. Se recomienda para empresas medianas y grandes. Para obtener más información acerca de Enterprise Management, consulte **Guía de usuario de Enterprise Management**.

Diferencias entre IAM y Enterprise Management

- Método de habilitación
  - IAM es gratuito y puede usarlo inmediatamente después de registrarse en Huawei Cloud.
  - Enterprise Management es un servicio de gestión de recursos en Huawei Cloud. Después de registrarse en el sistema, debe solicitar la habilitación de Enterprise Management. Para obtener más información, consulte **Habilitación de centro empresarial**.
- Aislamiento de recursos
  - Con IAM, puede crear varios proyectos en una región para aislar recursos y autorizar a los usuarios a acceder a recursos en proyectos específicos. Para obtener más información, consulte **Proyectos**.
  - Mediante Enterprise Management, puede crear proyectos de empresa para aislar recursos en distintas regiones. Enterprise Management le facilita la asignación de

permisos para recursos específicos en la nube. Por ejemplo, puede agregar un Elastic Cloud Server (ECS) a un proyecto empresarial y asignar permisos a un usuario para gestionar el ECS en el proyecto. El usuario entonces solo puede gestionar este ECS.

- Servicios compatibles
  - Para obtener más información sobre los servicios soportados por IAM, **Servicios en la nube admitidos**.
  - Para obtener más información sobre los servicios admitidos por Enterprise Management, consulte **Servicios en la nube admitidos**.

Relación entre la gestión empresarial y la IAM

- Las funciones de creación de usuarios y grupos de usuarios son las mismas para IAM y Enterprise Management.
- Si ha habilitado Enterprise Management, debe usar las políticas gestionadas en IAM para asignar permisos a los grupos de usuarios creados en Enterprise Management. Si las políticas definidas por el sistema no pueden cumplir sus requisitos, puede crear políticas personalizadas en IAM. Las políticas personalizadas se sincronizarán con Enterprise Management y se pueden asociar a grupos de usuarios tanto en IAM como en Enterprise Management.
- Si otorga a un grupo de usuarios permisos tanto en IAM como en Enterprise Management, los usuarios del grupo tendrán permisos de las políticas adjuntas al grupo tanto en IAM como en Enterprise Management. Las solicitudes de estos usuarios se autenticarán en función de las acciones de las políticas asociadas.
  - Si las políticas adjuntas contienen la misma acción, el efecto de la acción en IAM tiene prioridad. Por ejemplo, cuando un usuario solicita crear un servidor en la nube, se aplica el efecto Deny definido en IAM. Por lo tanto, el usuario no puede crear servidores en la nube.

```
A policy attached in an IAM project contains the following action:
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Deny"
}

A policy attached in an enterprise project contains the following action:
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Allow"
}
```

  - Todas las diferentes acciones en las políticas adjuntas en IAM y Enterprise Management entrarán en vigor. Las siguientes son dos acciones que permiten a los usuarios crear y eliminar servidores en la nube.

```
A policy attached in an IAM project contains the following action:
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Allow"
}
A policy attached in an enterprise project contains the following action:
{
  "Action": [
    "ecs:cloudServers:delete"
  ],
```

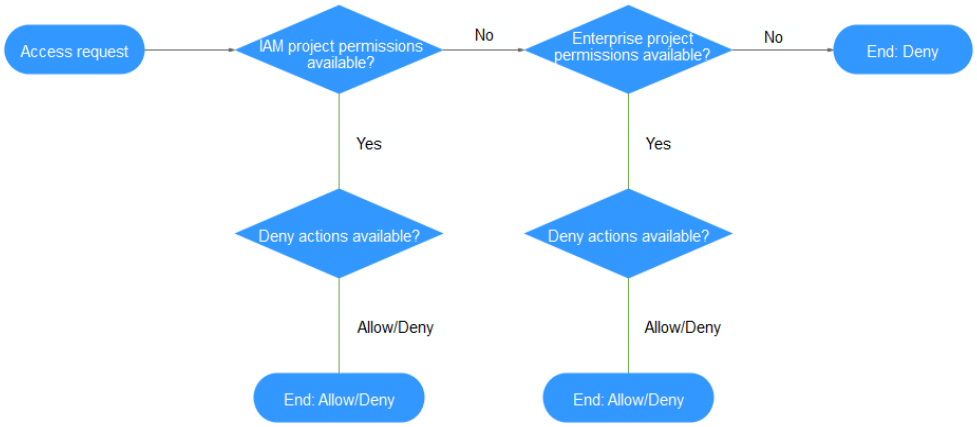


```
  "Effect": "Allow"
}
```

Proceso de autenticación

Cuando un usuario inicia una solicitud de acceso, el sistema autentica la solicitud basándose en las acciones de las políticas asociadas al grupo al que pertenece el usuario. La siguiente figura muestra el proceso de autenticación.

Figura 5-1 Proceso de solicitud de autenticación



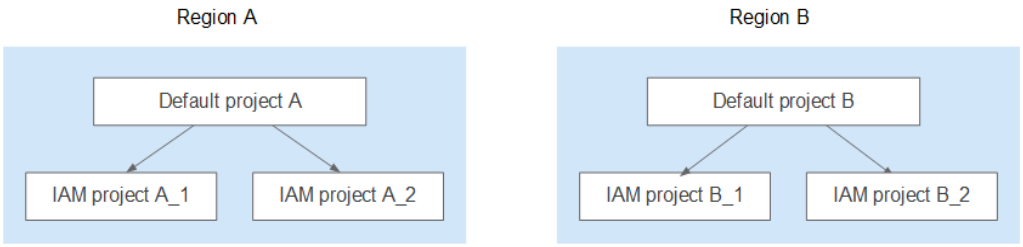
1. Un usuario inicia una solicitud de acceso.
2. El sistema busca permisos de proyecto de IAM y, a continuación, busca acciones coincidentes en los permisos.
3. Si se encuentra una acción coincidente Allow o Deny, el sistema devuelve un resultado de autenticación (Allow o Deny). A continuación, se completa la autenticación.
4. Si no se encuentran acciones coincidentes en los permisos de proyecto de IAM, el sistema continúa buscando permisos de proyecto de empresa y acciones coincidentes.
5. Si se encuentra una acción coincidente Allow o Deny, el sistema devuelve un resultado de autenticación (Allow o Deny). A continuación, se completa la autenticación.
6. Si no se encuentran acciones coincidentes, el sistema devuelve un Deny. A continuación, se completa la autenticación.

5.2 ¿Cuáles son las diferencias entre los proyectos de IAM y los proyectos empresariales?

Proyectos de IAM

Los proyectos de IAM agrupan y aíslan físicamente recursos en la misma región. Los recursos no se pueden transferir entre proyectos de IAM, pero solo se pueden eliminar y luego crear o comprar de nuevo.

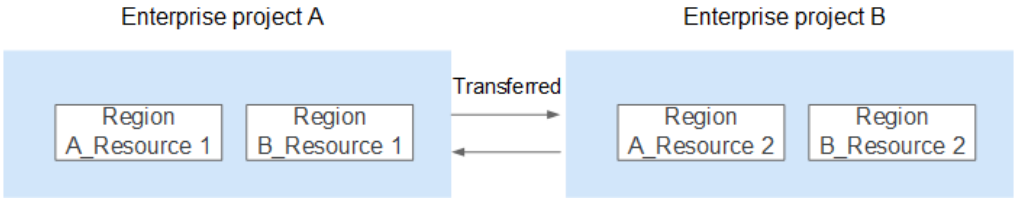
Para obtener más información sobre los proyectos de IAM, consulte **Proyectos**.



Proyectos empresariales

Los proyectos empresariales agrupan y gestionan recursos en distintas regiones. Los recursos de los proyectos empresariales están lógicamente aislados entre sí. Un proyecto de empresa puede contener recursos en varias regiones y los recursos se pueden transferir entre proyectos de empresa. Enterprise Management le facilita la asignación de permisos para recursos específicos en la nube. Por ejemplo, puede agregar un Elastic Cloud Server (ECS) a un proyecto empresarial y asignar permisos a un usuario para gestionar el ECS en el proyecto. El usuario entonces solo puede gestionar este ECS. No se pueden crear proyectos de IAM después de habilitar la gestión empresarial.

Para obtener más información sobre los proyectos de empresa, consulte **Creación de proyecto empresarial**.



5.3 ¿Cuáles son las diferencias entre los usuarios de IAM y las cuentas de miembros empresariales?

Usuarios de IAM

Los usuarios de IAM se crean mediante una cuenta en IAM o Enterprise Management (página **User Management**). Son gestionados y permisos concedidos por la cuenta. **Las facturas generadas por el uso de recursos por parte de los usuarios de IAM son pagadas por la cuenta.**

En una empresa, si hay varios empleados que necesitan usar los recursos adquiridos en Huawei Cloud a través de una cuenta, la cuenta se puede usar para crear usuarios de IAM para estos empleados y asignar permisos a los usuarios para usar los recursos. Los usuarios de IAM tienen sus propias contraseñas para acceder a los recursos de la cuenta.

Para obtener más información sobre cómo crear un usuario de IAM, consulte **Creación de un usuario**.

Cuentas de miembros de empresa

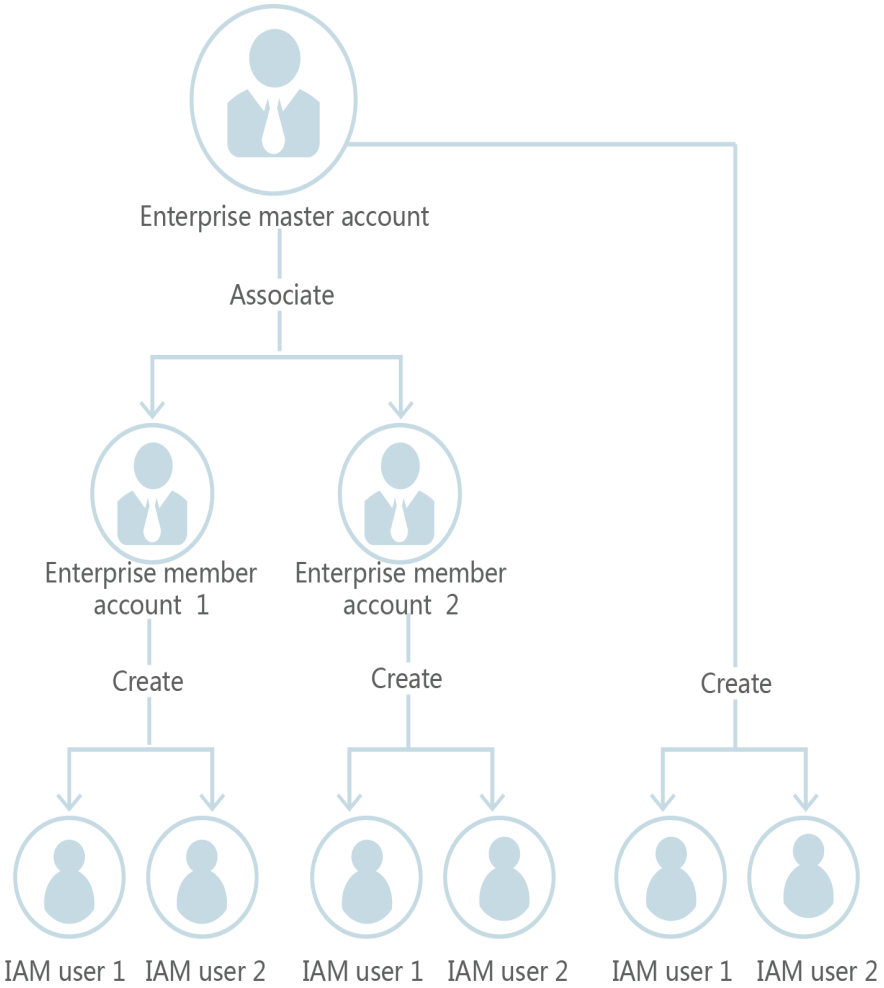
Tanto las cuentas maestras empresariales como cuentas de miembro se generan tras el registro exitoso en Huawei Cloud. **Accounting Management** de Enterprise Management permite asociar varias cuentas de Huawei Cloud entre sí con fines contables. Puede crear una

organización jerárquica y una cuenta maestra, agregar cuentas de miembro a esta organización y asociarlas con la cuenta maestra.

La cuenta maestra puede asignar fondos a cuentas de miembro para que la cuenta de miembro pueda usar los fondos para **gestionar recursos**.

Tanto la cuenta maestra como cuentas de miembro pueden crear usuarios de IAM. La cuenta maestra solo puede gestionar sus propios usuarios de IAM y no puede gestionar los usuarios de IAM de las cuentas de miembro.

Para obtener más información sobre cómo crear una cuenta de miembro, consulte **Creación de una cuenta de miembro**.



6 Gestión de delegación

6.1 ¿Cómo puedo obtener permisos para crear una agencia?

Síntoma

No tiene permisos para crear una agencia en la consola de IAM.

Causas posibles

No tiene permisos para utilizar IAM.

Solo los siguientes usuarios pueden usar IAM:

- 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 asignaron el rol **Security Administrator** o una política de **xxx FullAccess** (con permisos para acceder a IAM)

Soluciones

- Póngase en contacto con el administrador para crear una agencia. Para obtener más información, consulte **Creación de una delegación (por parte delegada)**.
- Póngase en contacto con el administrador para concederle los permisos para usar IAM. Para obtener más información, consulte **Asignación de permisos a un usuario de IAM**.

7 Gestión de cuentas

7.1 ¿Por qué falla el inicio de sesión de la cuenta?

Síntoma

Cuando inicia sesión en IAM con una cuenta, el sistema muestra un mensaje que indica que el nombre de cuenta o la contraseña son incorrectos.

Causas posibles

- El enlace de inicio de sesión es incorrecto.
- El ID de inicio de sesión es incorrecto.
- La contraseña es incorrecta.

Soluciones

- Utilice el enlace de inicio de sesión correcto e ingrese un ID de HUAWEI o una cuenta de Huawei Cloud. Si ya has actualizado tu cuenta a un ID de HUAWEI, elige **HUAWEI ID**, como se muestra en la sección **Figura 7-1**. De lo contrario, elija **Huawei Cloud Account**, como se muestra en **Figura 7-2**.
  - Para iniciar sesión con una cuenta de sitio web oficial de Huawei o como socio empresarial de Huawei o como usuario federado, consulte **Iniciar sesión en Huawei Cloud**.
  - Si es usuario de IAM, inicie sesión eligiendo **IAM User** en la página de inicio de sesión. Si el inicio de sesión falla, consulte **2.1 ¿Por qué falla el inicio de sesión de usuario de IAM?**.

Figura 7-1 Iniciar sesión con un ID de HUAWEI

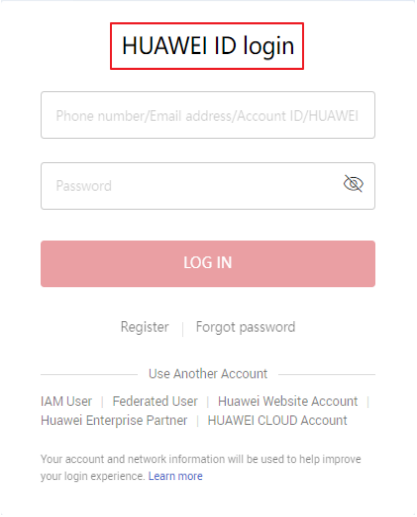
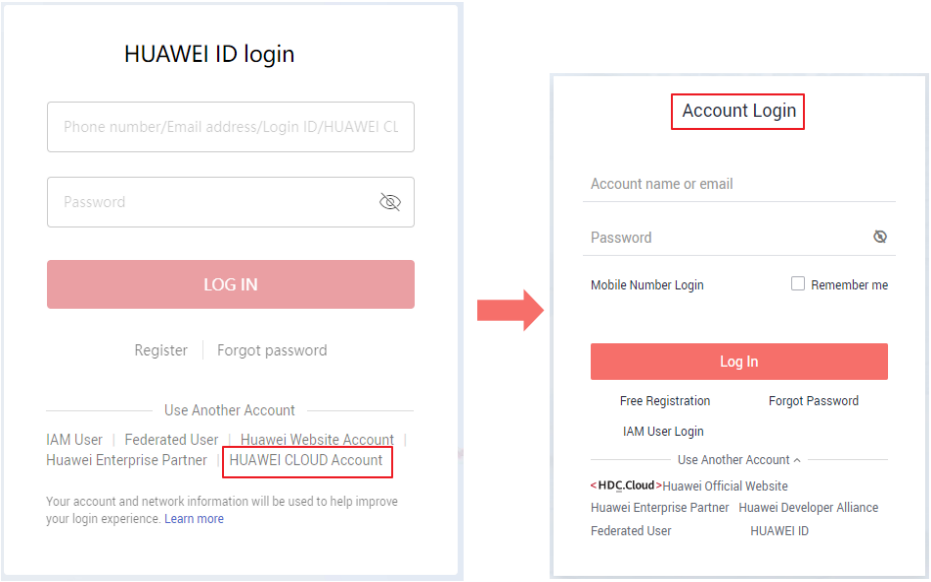


Figura 7-2 Iniciar sesión con una cuenta de Huawei Cloud



- Cuando inicie sesión con un ID de Huawei, ingrese el **número de teléfono móvil, dirección de correo electrónico, ID de inicio de sesión o nombre de cuenta de Huawei Cloud**. Cuando inicie sesión con una cuenta de Huawei Cloud, ingrese el **nombre o dirección de correo electrónico de la cuenta**.
  - Si tiene un ID de HUAWEI, ingrese el número de teléfono móvil o la dirección de correo electrónico asociada con el ID de HUAWEI, o ingrese el ID de inicio de sesión de este ID de HUAWEI. Para obtener más información, consulte **Iniciar sesión con un ID de HUAWEI**.
  - Si no tiene un ID de HUAWEI pero tiene una cuenta de Huawei Cloud, que no se ha actualizado a un ID de HUAWEI, introduzca el nombre de la cuenta de Huawei Cloud.
- Si inicia sesión con un ID de HUAWEI, introduzca la contraseña del ID de HUAWEI. Si inicia sesión con una cuenta de Huawei Cloud, introduzca la contraseña de la cuenta de Huawei Cloud.

7.2 ¿Cuáles son las relaciones entre una cuenta de Huawei Cloud, el ID de HUAWEI, el usuario de IAM y el usuario federado?

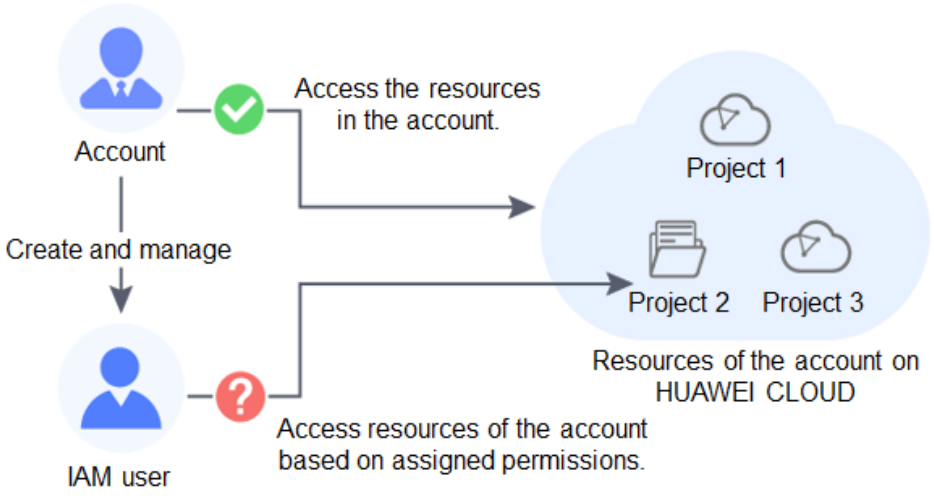
Esta sección presenta las cuentas utilizadas en Huawei Cloud y sus relaciones.

Tipos de cuenta de Huawei Cloud

El sistema de cuentas de Huawei Cloud consta de dos tipos de cuentas:

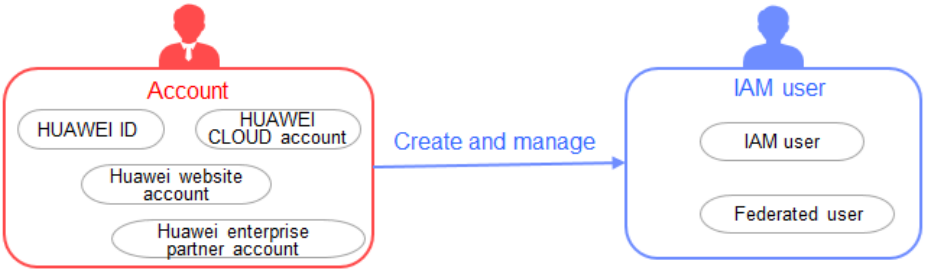
- **Accounts**: registrado o creado en Huawei Cloud. Una cuenta tiene los permisos más altos en Huawei Cloud. Puede acceder a todos sus recursos y paga por el uso de estos recursos. Las cuentas incluyen ID de Huawei y cuentas de Huawei Cloud.
- **IAM users**: creado y gestionado mediante una cuenta en IAM. El administrador de la cuenta otorga permisos a los usuarios de IAM y realiza el pago por los recursos que utilizan. Los usuarios de IAM usan recursos según lo especificado por los permisos.

Una cuenta y sus usuarios de IAM comparten una relación padre-hijo.



Puede iniciar sesión en Huawei Cloud con un ID de HUAWEI, una cuenta de sitio web de Huawei, una cuenta de socio empresarial de Huawei, o una cuenta de Huawei Cloud, y usar sus recursos y servicios en la nube.

Si es un usuario de IAM creado por una cuenta o un usuario de un sistema de terceros que ha establecido una relación de confianza con Huawei Cloud, inicie sesión en Huawei Cloud a través de la página correspondiente y, a continuación, utilice recursos y servicios en la nube según lo especificado por los permisos otorgados por la cuenta.

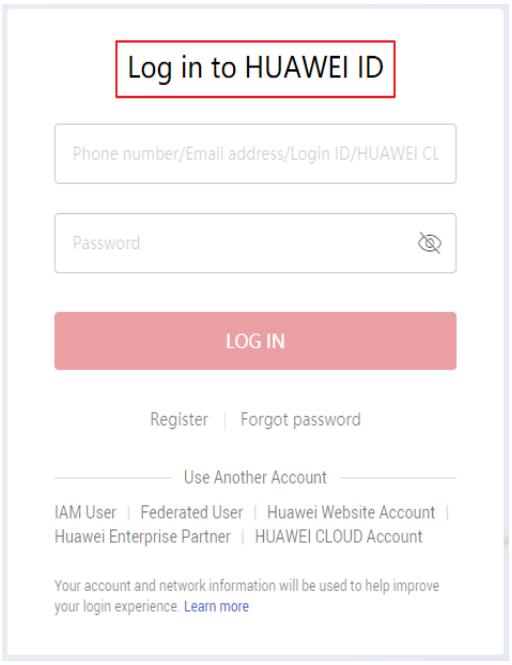


HUAWEI ID

Puede registrar un ID de HUAWEI para acceder a todos los servicios de Huawei, como Huawei Cloud y Vmall.

Registration: Registre un ID de HUAWEI en cualquier sitio web de servicio de Huawei, como el **sitio web de ID de Huawei**.

Huawei Cloud login: Inicie sesión en Huawei Cloud haciendo clic en **HUAWEI ID**. Si es la primera vez que inicias sesión en Huawei Cloud con un ID de HUAWEI, habilita los servicios de Huawei Cloud o vincula el ID de Huawei a su cuenta de Huawei Cloud siguiendo las indicaciones en pantalla.

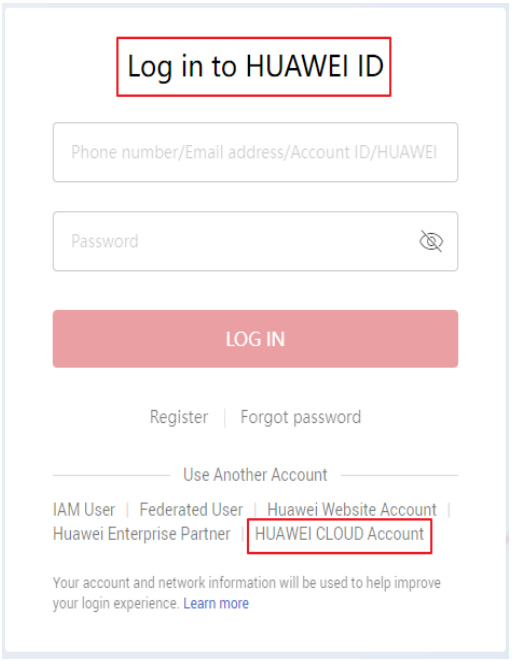


Cuenta de Huawei Cloud

Las cuentas de Huawei Cloud solo se pueden usar para iniciar sesión en Huawei Cloud.

Registration: Para mejorar la experiencia de inicio de sesión, hemos unificado nuestro sistema de cuentas. Solo puede registrar los ID de HUAWEI en Huawei Cloud a partir del 30 de octubre de 2021.

HUAWEI CLOUD login: Inicie sesión en Huawei Cloud haciendo clic en **HUAWEI ID** o **HUAWEI CLOUD Account**.

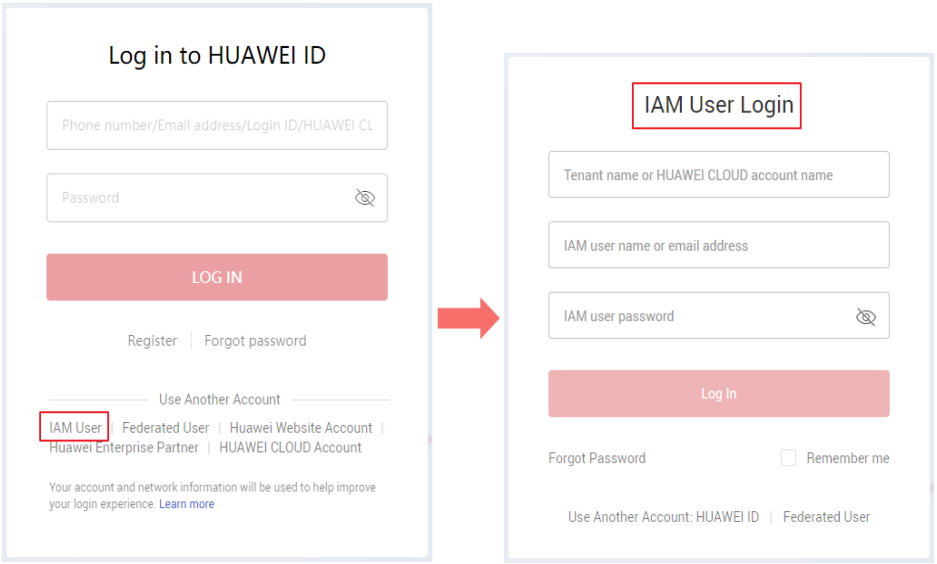


Usuario de IAM

Los usuarios de IAM utilizan los recursos de Huawei Cloud según lo especificado por los permisos otorgados por su cuenta.

Creation: Los usuarios de IAM son creados por una cuenta en IAM. Para obtener más información, consulte **Creación de un usuario de IAM**.

Huawei Cloud login: Inicie sesión en Huawei Cloud haciendo clic en **IAM User**.

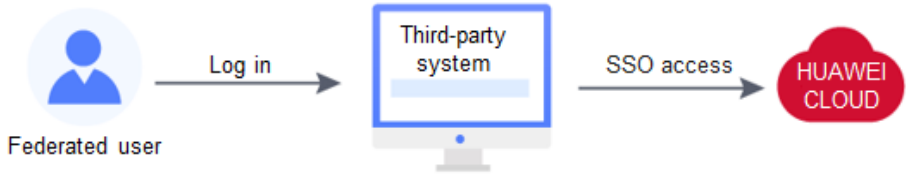


Usuario federado (usuario virtual de IAM)

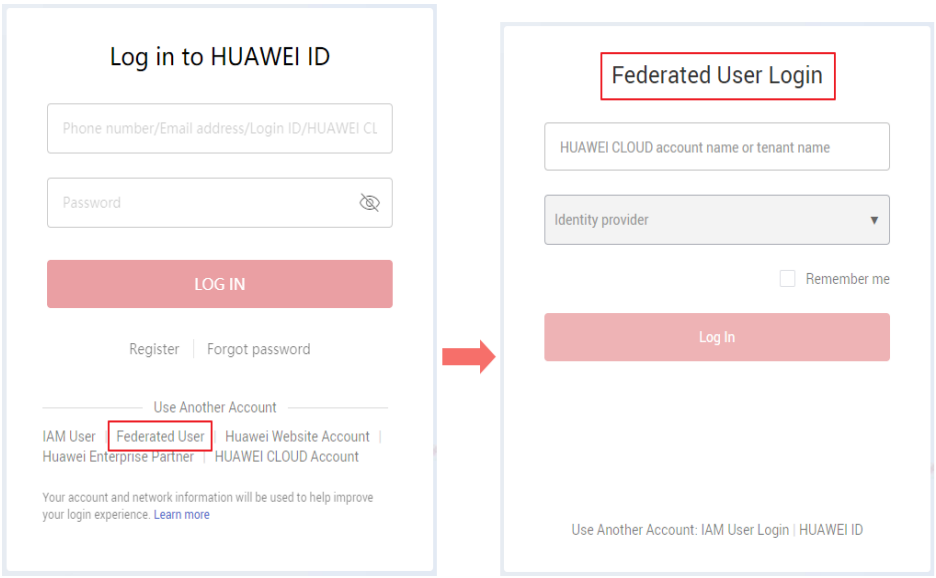
Los usuarios federados están registrados en un sistema de terceros que ha establecido una relación de confianza con Huawei Cloud. Los usuarios pueden iniciar sesión en Huawei

Cloud utilizando cuentas de sistema de terceros. Por ejemplo, pueden iniciar sesión en una plataforma de juegos usando sus cuentas de servicio de redes sociales (SNS).

Creation: Cuando un usuario empresarial inicia sesión en Huawei Cloud con una cuenta de un sistema de terceros, IAM crea automáticamente un usuario IAM virtual (usuario federado empresarial). El sistema de terceros corresponde a un proveedor de identidad que ha creado en IAM. Para obtener más información, consulte **Introducción a proveedor de identidad**.



Huawei Cloud login: Inicie sesión en Huawei Cloud haciendo clic en **Federated User**.



Otros

Si ya tiene una **cuenta de sitio web de Huawei** o una **cuenta de socio empresarial de Huawei**, inicie sesión en Huawei Cloud con estas cuentas y use recursos como administrador de cuentas.

7.3 ¿Cuáles son las posibles causas de una falla de actualización de ID de HUAWEI?

Síntoma

Su cuenta de Huawei Cloud no se puede actualizar a un ID de HUAWEI.

Causas posibles

1. Ha registrado una cuenta de Huawei Cloud y un ID de HUAWEI con el mismo número de teléfono móvil o dirección de correo electrónico, y no ha utilizado el ID de HUAWEI para habilitar los servicios de Huawei Cloud.

   Cierre la sesión de su cuenta de Huawei Cloud, vuelva a iniciar sesión con su ID de HUAWEI y asocie la cuenta con el ID.

2. Ha registrado **multiple** cuentas de Huawei Cloud y **one** ID de HUAWEI, y ha asociado una de las cuentas con el ID. En este caso, no puede asociar otra cuenta de Huawei Cloud con su ID de HUAWEI.

   Inicie sesión con su cuenta Huawei Cloud e ignore el aviso de actualización durante el inicio de sesión.

3. Ha registrado una cuenta de Huawei Cloud y un ID de HUAWEI en diferentes países o regiones con el mismo número de teléfono móvil o dirección de correo electrónico. En este caso, no puede asociar la cuenta con el ID.

   Inicie sesión con su cuenta Huawei Cloud e ignore el aviso de actualización durante el inicio de sesión.

4. Su ID de HUAWEI está congelado.

   Vaya al **HUAWEI ID website > Security center > Unfreeze account** para descongelar su cuenta e inténtelo de nuevo.

5. Su número de móvil ya se ha utilizado para registrar un ID de HUAWEI.

   Registre un nuevo ID de HUAWEI en el **sitio web de ID de HUAWEI** y asocie su cuenta de Huawei Cloud con el nuevo ID.

7.4 ¿Puedo iniciar sesión con mi cuenta Huawei Cloud después de actualizarla a un ID de HUAWEI?

- **Si ya ha registrado un ID de HUAWEI:**

  Si el número de teléfono móvil, la dirección de correo electrónico y el ID de inicio de sesión de su ID de HUAWEI son los mismos que los de su cuenta de Huawei Cloud, puede iniciar sesión con la cuenta. Si los números de teléfono móvil son los mismos pero las direcciones de correo electrónico son diferentes, solo puede iniciar sesión con el número de teléfono móvil de la cuenta de Huawei Cloud.

- **Si nunca ha registrado un ID de HUAWEI:**

  Después de la actualización, puede iniciar sesión con el mismo número de teléfono móvil, dirección de correo electrónico o nombre de cuenta.

8 Otros

8.1 ¿Cómo obtengo un token de usuario usando Postman?

Postman es una herramienta de edición visual para crear y probar solicitudes de API. Proporciona una interfaz de usuario fácil de usar para enviar solicitudes HTTP, incluidas solicitudes GET, PUT, POST y DELETE. Postman le permite modificar los parámetros de las solicitudes HTTP y devuelve la respuesta a sus solicitudes.

Un token es la credencial de acceso de un usuario, que incluye identidades y permisos de usuario. Cuando se invoca a una API para acceder a los recursos de la nube, se requiere un token para la autenticación de identidad.

Realice el procedimiento descrito en esta sección para obtener un token de usuario mediante Postman. Para obtener más información sobre los parámetros, consulte **Obtención de un token de usuario**.

NOTA

- **Período de validez de un token**

  El período de validez de un token es de **24 hours**. Almacenar en caché el token para evitar invocaciones frecuentes a la API. Asegúrese de que el token es válido mientras lo usa. El uso de un token que caducará pronto puede provocar fallas en las invocaciones a la API.

  La obtención de un nuevo token no afecta a la validez del token existente. Sin embargo, las siguientes operaciones invalidarán el token existente:

  - Eliminar o deshabilitar el usuario de IAM
  - Cambio de la contraseña o clave de acceso del usuario de IAM
  - Se cambian los permisos del usuario de IAM (debido a pagos pendientes, aprobación de la solicitud OBT o modificación del permiso).
- **Obtención de un token**
  - Si su cuenta de Huawei Cloud se ha actualizado a un ID de HUAWEI, no puede obtener un token con el ID de HUAWEI. Sin embargo, puede crear un usuario de IAM, conceder al usuario los permisos necesarios y obtener un token como usuario.
  - Si es usuario de un sistema de terceros, no puede obtener un token utilizando el nombre de usuario y la contraseña que utiliza para la autenticación de identidad federada. Vaya a la página de inicio de sesión de Huawei Cloud, haga clic en **Forgot password**, haga clic en **Reset HUAWEI CLOUD account password** y establezca una contraseña.

Prerrequisitos

Ha instalado y registrado en Postman.

NOTA

- Se recomienda instalar una versión de Postman que admita un encabezado superior a 32 KB. De lo contrario, se puede informar de un error de desbordamiento de cabecera.

Procedimiento

Paso 1 Edite la URL de solicitud, el encabezado y el cuerpo de la API utilizada para obtener un token para invocar a las API.

- **URL de solicitud**

  El URL de la solicitud tiene el formato "**https://***IAM region and endpoint*/*API URI*".

  a. Obtenga la región y el punto de conexión de IAM de **Regiones y puntos de conexión**.

  Figura 8-1 Regiones y puntos de conexión de IAM

  Identity and Access Management (IAM)

Region Name	Region	Endpoint	Protocol Type
AF-Johannesburg	af-south-1	iam.af-south-1.myhuaweicloud.com	HTTPS
ALL	ALL	iam.myhuaweicloud.com	HTTPS
AP-Bangkok	ap-southeast-2	iam.ap-southeast-2.myhuaweicloud.com	HTTPS
AP-Hong Kong	ap-southeast-1	iam.ap-southeast-1.myhuaweicloud.com	HTTPS
AP-Singapore	ap-southeast-3	iam.ap-southeast-3.myhuaweicloud.com	HTTPS

  b. Obtener el URI de la API a partir de la **Obtención de un token de usuario**.

  Por ejemplo, la URL de solicitud en la región **ap-southeast-1** es **https://iam.ap-southeast-1.myhwclouds.com/v3/auth/tokens**.

c. Seleccione un método de solicitud de API e ingrese la URL de solicitud en Postman.

- **Encabezado de solicitud**

  Establezca **key** en **Content-Type** y **value** en **application/json;charset=utf8**.

- **Cuerpo de solicitud**

  Modifique los parámetros en el cuerpo de la solicitud de ejemplo.

```
{
    "auth": {
        "identity": {
            "methods": [
                                "password"
                            ],
            "password": {
                "user": {
                    "domain": {
                        "name": "Account name"
                    },
                    "name": "IAM user name",
                    "password": "IAM user password"
                }
            }
        },
        "scope": {
            "domain": {
                "name": "Account name"
            }
        }
    }
}
```

NOTA

Para obtener más información sobre cómo obtener el nombre de cuenta y el nombre de usuario de IAM, consulte **Obtención de cuenta, usuario de IAM e información de proyecto**.

Paso 2 Haga clic en **Send** para enviar la solicitud de API.

Paso 3 Vea el token en el encabezado de respuesta. Puede usar este token para la autenticación cuando invoque a otras API de IAM.

NOTA

- Si se devuelve el error **401**, la autenticación ha fallado. Asegúrese de que los parámetros en el cuerpo de la solicitud son correctos y envíe la solicitud de nuevo.
- Si se devuelve el error **400**, el formato del cuerpo es incorrecto. Compruebe si el formato de cuerpo cumple con la sintaxis JSON. Para obtener más información, consulte **Códigos de estado**.
- Si se muestra "Header Overflow", resuelve el problema haciendo referencia a **¿Por qué veo un mensaje que indica Header Overflow cuando intento usar Postman para obtener un token?**

----Fin

¿Por qué veo un mensaje que indica Header Overflow cuando intento usar Postman para obtener un token?

Postman de V7.25.0, V7.26.0 o una versión posterior no se puede utilizar para obtener un token de usuario debido a las configuraciones. El mensaje "Header Overflow" se mostrará si utiliza cualquiera de estas versiones.

- **Solución 1**

  Utilizar una versión anterior de Postman, como V 5.xx.

- **Solución 2:**

  Utilizar curl para obtener un token y reemplazar el texto en negrita con valores reales:

  ```
  curl -ik -X POST -H 'Content-Type=application/json;charset=utf8' -d '{"auth": {"identity": {"methods": ["password"],"password": {"user": {"domain": {"name": "Account name"},"name": "IAM username","password": "IAM user password"}}},"scope": {"domain": {"name": "Account name"}}}}' https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
  ```

- **Solución 3**

  Pasar una variable de entorno adicional **NODE_OPTIONS=--max-http-header-size=16384 (16KB)** a Postman para especificar el tamaño máximo del encabezado HTTP (en bytes).

  Ejecutar uno de los siguientes comandos dependiendo de su sistema operativo:

  - macOS

    ```
    NODE_OPTIONS=--max-http-header-size=16384 /Applications/Postman.app/Contents/MacOS/Postman
    ```

  - Linux

    ```
    NODE_OPTIONS=--max-http-header-size=16384 /path/to/Postman/Postman
    ```

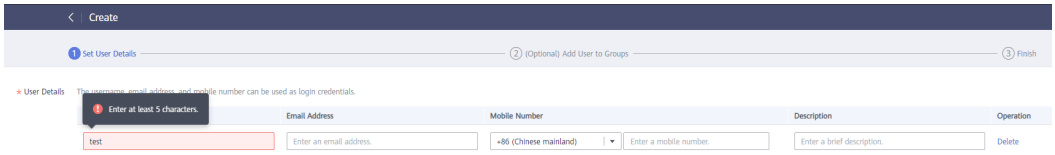
  - Windows

    ```
    set NODE_OPTIONS=--max-http-header-size=16384
    C:\users\<username>\AppData\local\Postman\Postman.exe
    ```

8.2 ¿Por qué siempre se muestra la ayuda a nivel de campo?

Cuando se registra o inicia sesión en Huawei Cloud, vincule una cuenta de Huawei Cloud, cree un usuario, o restablezca o cambie la contraseña, ayuda a nivel de campo, como "Enter at least 5 characters." siempre se muestra porque puede estar utilizando Internet Explorer 8 o una versión anterior. En este caso, solucione el problema utilizando los siguientes métodos.

Figura 8-2 La ayuda a nivel de campo siempre se muestra



- Actualice el navegador.

  Actualice a Internet Explorer 9 o una versión posterior.

- Use otro navegador.

  Utiliza Mozilla Firefox (versión 38.0 o posterior) o Google Chrome (versión 43.0 o posterior).

8.3 ¿Cómo puedo desactivar la contraseña de relleno automático en Google Chrome?

Cuando utilice Google Chrome para iniciar sesión en Huawei Cloud por primera vez, aparecerá un mensaje pidiéndole que confirme si quiere guardar la contraseña. Esto se debe a

que **Offer to save passwords** y **Auto Sign-in** en el área **Passwords** de la página **Settings** en Google Chrome se seleccionan de forma predeterminada después de instalar el navegador Google Chrome. Si confirma guardar la contraseña, la contraseña se llenará automáticamente durante su próximo inicio de sesión. Para garantizar la seguridad de su cuenta y contraseña, realice las siguientes operaciones para desactivar esta función. Esta sección utiliza Google Chrome 61.0.3163.100 como ejemplo para describir cómo deshabilitar esta función.

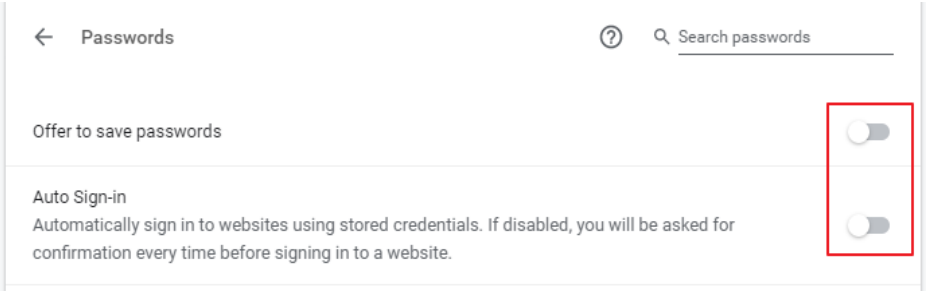
Procedimiento

Paso 1 Abra el navegador Google Chrome, haga clic en en la esquina superior derecha del navegador y elija **Settings**.

Paso 2 En el área **Autofill**, haga clic en **Passwords**.

Paso 3 Anule la selección de **Offer to save passwords** y **Auto Sign-in**.

Figura 8-3 Anular la selección de Offer to save passwords y Auto Sign-in.



----Fin

Procedimiento de seguimiento

Para eliminar una contraseña guardada, en el área **Saved Passwords**, haga clic en junto a la contraseña y haga clic en **Remove**. Se eliminará la contraseña.

8.4 Región y AZ

Concepto

Una región y una zona de disponibilidad (AZ) identifican la ubicación de un centro de datos. Puede crear recursos en una región específica y AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- Una zona AZ es una ubicación física en la que los recursos utilizan fuentes de alimentación y redes independientes. Una región contiene una o más AZ que están físicamente aisladas pero interconectadas a través de redes internas. Debido a que las AZ están aisladas entre sí, cualquier fallo que ocurra en una AZ no afectará a otras.
- Las regiones se dividen en función de la ubicación geográfica y la latencia de la red. Los servicios públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS),

Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) y Image Management Service (IMS), se comparten dentro de la misma región. Las regiones se clasifican en regiones universales y regiones dedicadas. Una región universal proporciona servicios en la nube universales para los tenants estándares. Una región dedicada proporciona servicios específicos para tenants específicos.

- Una AZ contiene uno o más centros de datos físicos. Cada AZ cuenta con instalaciones independientes de electricidad, de refrigeración, de extinción de incendios y a prueba de humedad. Dentro de una AZ, los recursos de computación, red, almacenamiento y otros se dividen de forma lógica en múltiples clústeres. Las AZ dentro de una región están interconectadas usando fibras ópticas de alta velocidad, para soportar sistemas de alta disponibilidad entre las AZ.

Figura 8-4 Figura 8-5 muestra la relación entre regiones y AZ.

Figura 8-4 Las regiones y las AZ

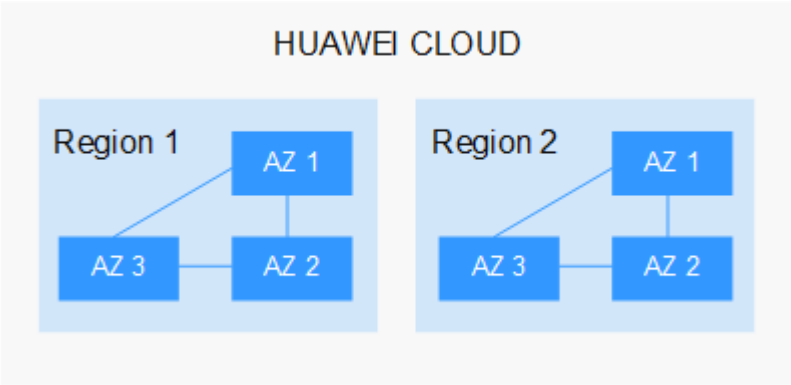
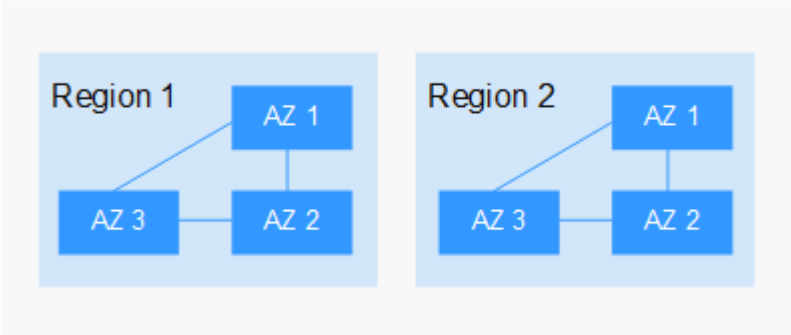


Figura 8-5 Regions and AZs



Huawei Cloud ofrece servicios en muchas regiones de todo el mundo. Seleccione una región y AZ según los requisitos. Para obtener más información, consulte **Regiones globales de Huawei Cloud**.

Selección de una región

Al seleccionar una región, tenga en cuenta los siguientes factores:

- Localización

  Se recomienda seleccionar la región más cercana para una menor latencia de red y un acceso rápido. Las regiones dentro de China continental proporcionan la misma infraestructura, calidad de red BGP, así como operaciones de recursos y configuraciones.

Por lo tanto, si sus usuarios objetivo están en China continental, no es necesario tener en cuenta las diferencias de latencia de la red al seleccionar una región.

- Si sus usuarios objetivo se encuentran en Asia Pacífico (excepto China continental), seleccione la región **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore**.
- Si sus usuarios objetivo se encuentran en África, seleccione la región **AF-Johannesburg**.
- Si sus usuarios objetivo están en América Latina, seleccione la región **LA-Santiago**.

  NOTA

  La región **LA-Santiago** se encuentra en Chile.

- Precio del recurso

  Los precios de los recursos pueden variar en diferentes regiones. Para obtener más información, consulte **Detalles de precios del producto**.

Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

Selección de una AZ

Al implementar recursos, tenga en cuenta los requisitos de las aplicaciones en cuanto a la recuperación ante desastres (DR) y la latencia de la red.

- Para una alta capacidad de DR, implemente recursos en diferentes AZ dentro de la misma región.
- Para una menor latencia de red, implemente recursos en la misma AZ.

Regiones y endpoint

Antes de usar una API para llamar a recursos, especifique su región y endpoint.

8.5 ¿Cómo solicito los permisos para acceder a recursos en una Región de la alianza en la nube usando mi cuenta de Huawei Cloud o el ID de HUAWEI?

Puede enviar un ticket de servicio para solicitar los permisos necesarios para acceder a recursos en regiones de alianza en la nube como **EU-Dublin**.

Procedimiento

Paso 1 **Envíe un ticket de servicio** y especifique la región de alianza en la nube a la que desea acceder.

Paso 2 Espere una notificación por correo electrónico de aprobación. Después de recibir el correo electrónico, **inicie sesión en la consola de gestión** y haga clic en  en la esquina superior izquierda para seleccionar la región a la que desea acceder.

----Fin

