# IAM

# Descripción general del servicio

**Edición** 01

**Fecha** 2022-11-20

**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**

### Marcas registradas y permisos

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

### Aviso

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

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

## Huawei Cloud Computing Technologies Co., Ltd.

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

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

# Índice



# 1 Infografías

# 2 ¿Qué es IAM?

Huawei Cloud Identity and Access Management (IAM) proporciona gestión de permisos para ayudarle a controlar de forma segura el acceso a sus servicios y recursos en la nube.

IAM es gratuito. Solo paga por los recursos en la nube de su cuenta.

## Ventajas

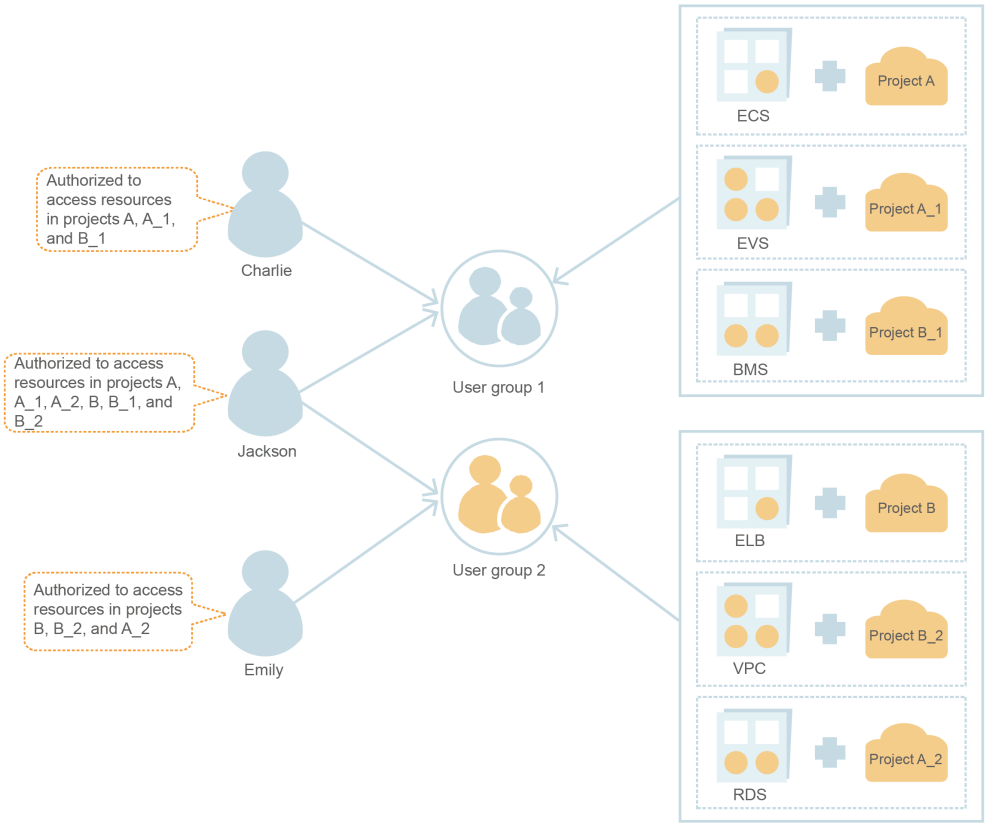
**Control de acceso detallado para los recursos de Huawei Cloud**

Cuando se registra correctamente en Huawei Cloud, su cuenta se crea automáticamente. Su cuenta tiene permisos de acceso completos para sus servicios y recursos en la nube y realiza pagos por el uso de estos recursos.

Si compra varios recursos de Huawei Cloud, como Elastic Cloud Servers (ECSs), Elastic Volume Services (EVSs), and Bare Metal Servers (BMSs), para diferentes equipos o aplicaciones en su empresa, puede utilizar su cuenta para crear usuarios de IAM para los miembros del equipo o las aplicaciones y concederles los permisos necesarios para completar tareas específicas. Los usuarios de IAM utilizan sus propios nombres de usuario y contraseñas para iniciar sesión en Huawei Cloud y acceder a los recursos de su cuenta.

Además de IAM, puede usar Enterprise Management para controlar el acceso a los recursos de la nube. Enterprise Management admite una gestión de permisos más detallada y una gestión de proyectos empresariales. Puede elegir entre IAM o Enterprise Management para satisfacer sus necesidades. Para obtener más información, consulte **¿Cuáles son las diferencias entre IAM y Enterprise Management?**

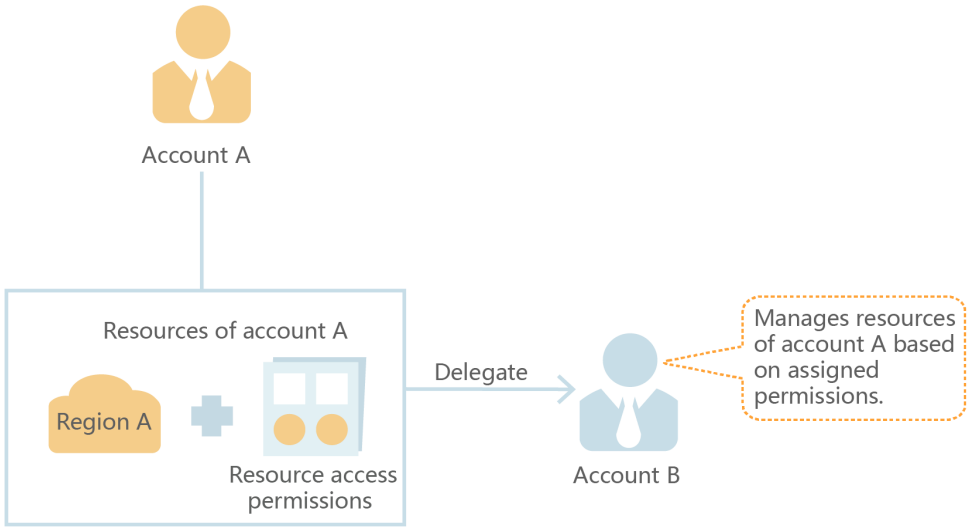
  




**Delegación de acceso a recursos entre cuentas**

Si compra varios recursos de Huawei Cloud, puede delegar otra cuenta para gestionar algunos de sus recursos para una operación eficiente.

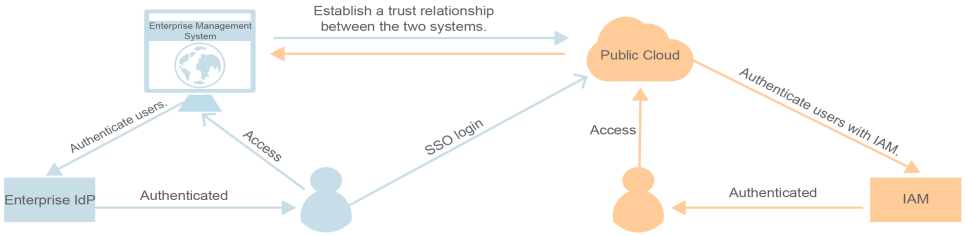
Por ejemplo, puede crear una agencia para una empresa profesional de O&M para permitir que la empresa administre recursos específicos con la propia cuenta de la empresa. Si la delegación cambia, puede modificar o revocar los permisos delegados en cualquier momento. En la siguiente figura, la cuenta A es la parte delegante y la cuenta B es la parte delegada.



**Acceso federado a Huawei Cloud con cuentas empresariales existentes (federación de identidades)**

Si su empresa tiene un sistema de identidad, puede crear un proveedor de identidad (IdP) en IAM para proporcionar acceso de inicio de sesión único (SSO) a Huawei Cloud para los empleados de su empresa. El proveedor de identidad establece una relación de confianza entre su empresa y Huawei Cloud, lo que permite a los empleados acceder a Huawei Cloud utilizando sus cuentas existentes.




## Métodos de acceso

Puede acceder a IAM utilizando cualquiera de los siguientes métodos:

- **Consola de gestión**

  Acceda a IAM a través de la consola de gestión ─ una interfaz visual basada en navegador. Para obtener más información, consulte **Acceso a la consola de IAM**.

- **Las API de REST**

  Acceda a IAM usando API REST de forma programable. Para obtener más información, consulte **Referencia de API**.

# 3 Conceptos básicos

Los siguientes son conceptos básicos que debe comprender antes de comenzar con el servicio IAM.

## Cuenta

Se crea una cuenta después de registrarse con éxito en Huawei Cloud. Su cuenta tiene permisos de acceso completos para sus recursos en la nube y realiza pagos por el uso de estos recursos. Puede utilizar la cuenta para restablecer las contraseñas de usuario y asignar permisos.

No puede modificar o eliminar su cuenta en IAM, pero puede hacerlo en My Account.

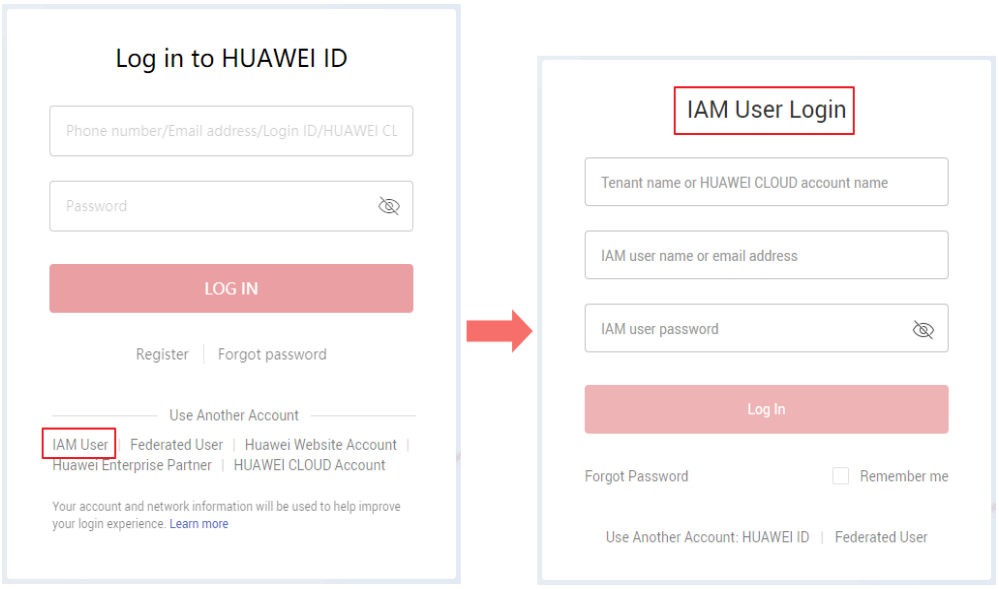
## Usuario de IAM

Puede usar su cuenta para crear usuarios de IAM y asignar permisos para recursos específicos. Cada usuario de IAM tiene sus propias credenciales de identidad (contraseñas o claves de acceso) y utiliza recursos en la nube basados en los permisos asignados. Los usuarios de IAM no pueden realizar pagos por sí mismos. Puede usar su cuenta para pagar sus facturas.

Si un usuario de IAM olvida su contraseña, puede restablecerla consultando **¿Cómo puedo restablecer mi contraseña?**

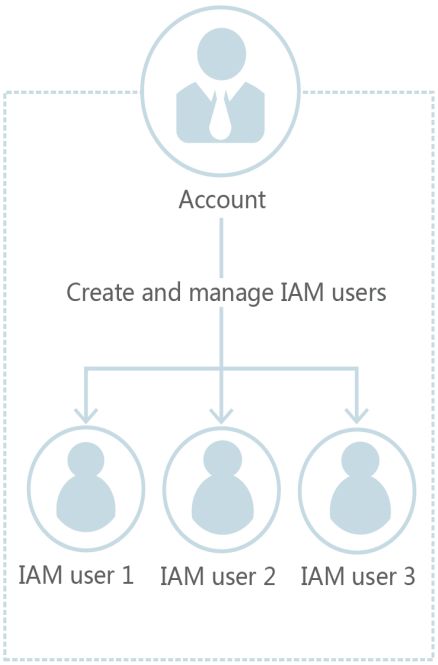
**Figura 3-1** Inicio de sesión de usuario de IAM




## Relación entre una cuenta y sus usuarios de IAM

Una cuenta y sus usuarios de IAM tienen una relación padre-hijo. La cuenta es propietaria de los recursos y realiza pagos por los recursos utilizados por los usuarios de IAM. Tiene permisos completos para estos recursos. Los usuarios de IAM son creados por una cuenta, y solo tienen los permisos otorgados por la cuenta. La cuenta puede modificar o revocar los permisos de los usuarios de IAM en cualquier momento.

**Figura 3-2** Usuarios de cuenta e IAM



## Autorización

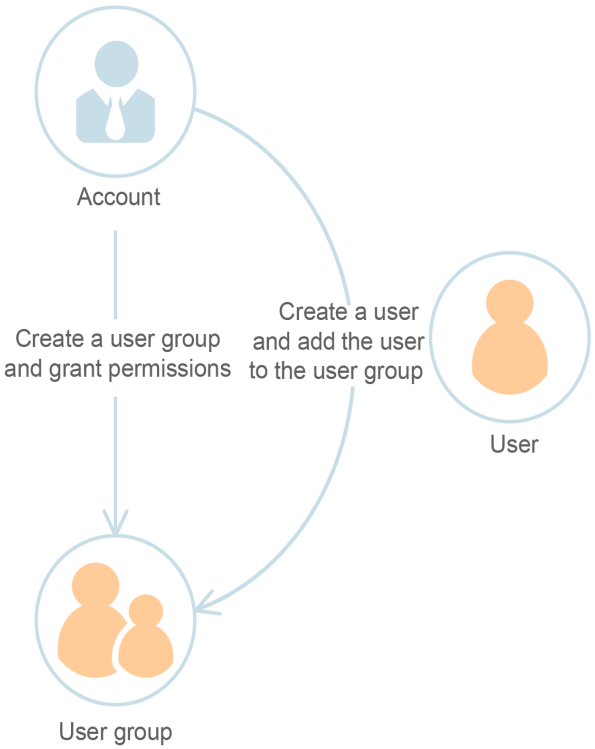
La autorización es el proceso de concesión de permisos necesarios para que un usuario realice tareas específicas.

## Grupo de usuario

Un grupo de usuarios de IAM es una colección de usuarios de IAM. Los grupos de usuarios permiten especificar permisos para varios usuarios, lo que puede facilitar la gestión de los permisos para esos usuarios. Los usuarios de IAM agregados a un grupo de usuarios obtienen automáticamente los permisos asignados al grupo. Si se agrega un usuario a varios grupos de usuarios, el usuario heredará los permisos de todos estos grupos.

Hay un grupo de usuarios predeterminado **admin**. Tiene todos los permisos necesarios para usar todos los recursos de la nube. Los usuarios de IAM de este grupo pueden realizar operaciones en todos los recursos, incluidas, entre otras, la creación de grupos de usuarios y usuarios, la asignación de permisos y la gestión de recursos.

**Figura 3-3** Grupo de usuarios y usuarios




## Permisos

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Una estrategia de autorización de grano grueso proporcionada por IAM para asignar permisos en función de las responsabilidades del trabajo de los usuarios. Solo un número limitado de roles de nivel de servicio están disponibles para autorización.
- Políticas: Una estrategia de autorización detallada que define los permisos necesarios para realizar operaciones en recursos específicos en la nube bajo ciertas condiciones. Este tipo de autorización es más flexible y es ideal para el acceso de privilegios mínimos.

Por ejemplo, puede conceder a los usuarios solo permiso para gestionar ECS de un tipo determinado. IAM admite políticas personalizadas y definidas por el sistema.

- Una **system-defined policy** define las acciones comunes de un servicio en la nube. Las políticas definidas por el sistema se pueden utilizar para asignar permisos a grupos de usuarios y no se pueden modificar. Si necesita asignar permisos para un servicio específico a un grupo de usuarios o delegación en la consola de IAM pero no puede encontrar las políticas correspondientes, indica que el servicio no admite la gestión de permisos a través de IAM. Puede **enviar un ticket de servicio** para solicitar que los permisos para el servicio estén disponibles en IAM.
- Las políticas personalizadas funcionan como complemento de las políticas definidas por el sistema. Puede crear políticas personalizadas utilizando las acciones admitidas por los servicios en la nube para un control de acceso más refinado. Puede crear políticas personalizadas en el editor visual o en la vista JSON.

**Figura 3-4** Permisos de ejemplo

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "apm:*:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

## Credenciales

Las credenciales confirman la identidad de un usuario cuando el usuario accede a Huawei Cloud a través de la consola o las API. Las credenciales pueden ser una contraseña o claves de acceso. Puede gestionar sus propias credenciales y las credenciales de los usuarios de IAM.

- Contraseña: Una credencial común para iniciar sesión en la consola de gestión o invocar a las API.
- Clave de acceso: Un par ID de clave de acceso/clave de acceso secreta (AK/SK), que solo se puede usar para invocar a las API. Cada clave de acceso proporciona una firma para la autenticación criptográfica para garantizar que las solicitudes de acceso sean secretas, completas y correctas.

## Dispositivo MFA virtual

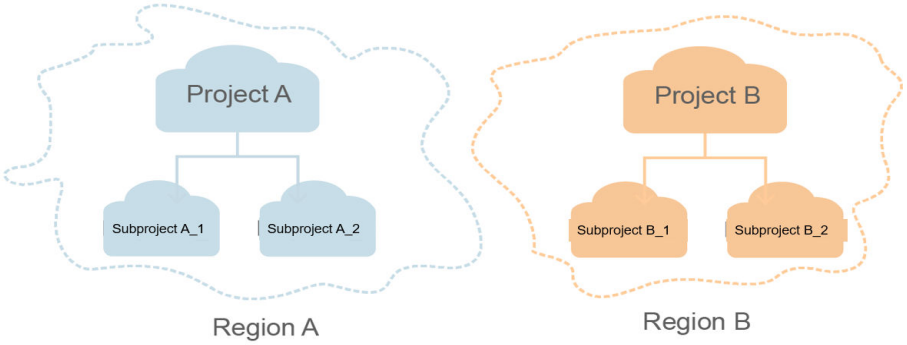
Un dispositivo MFA virtual es una aplicación que genera códigos de verificación de 6 dígitos de acuerdo con el estándar de Algoritmo de contraseña única basada en el tiempo (TOTP). Los dispositivos MFA pueden estar basados en hardware o software. Huawei Cloud solo admite dispositivos MFA virtuales basados en software, que son programas de aplicación que se ejecutan en dispositivos inteligentes como celulares. Para obtener más información acerca de cómo usar dispositivos MFA virtuales, consulte **Dispositivo MFA virtual**.

## Proyecto

Una región corresponde a un proyecto. Los proyectos predeterminados se definen para agrupar y aislar físicamente recursos (incluidos recursos informáticos, de almacenamiento y de red) entre regiones. Puede conceder permisos a los usuarios en un proyecto predeterminado para acceder a todos los recursos de la región asociada al proyecto. Si necesita un control de acceso más refinado, puede crear subproyectos con un proyecto predeterminado y comprar recursos en subproyectos. A continuación, puede asignar los permisos necesarios para que los usuarios accedan solo a recursos en subproyectos específicos.

**Figura 3-5** Proyectos




## Proyecto empresarial

Los proyectos empresariales le permiten agrupar y gestionar recursos entre regiones. Los recursos de los proyectos empresariales están lógicamente aislados entre sí. Un proyecto de empresa puede contener recursos de varias regiones y puede agregar recursos a proyectos de empresa o quitarlos fácilmente.

Para obtener más información acerca de cómo obtener los ID y características de proyecto empresarial, consulte la **Guía del usuario de Enterprise Management**.

## Delegación

Una relación de confianza que puede establecer entre su cuenta y otra cuenta o un servicio en la nube para delegar el acceso a recursos.

- Delegación de cuentas: puede delegar otra cuenta para implementar O&M en sus recursos en función de los permisos asignados.
- Delegación de servicios en la nube: Servicios de Huawei Cloud se interactúan entre sí, y algunos servicios en la nube dependen de otros servicios. Puede crear una agencia para delegar un servicio en la nube para acceder a otros servicios.

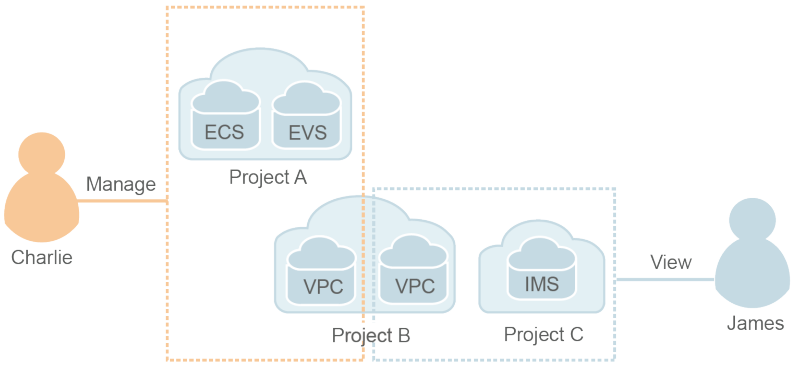
# 4 Funciones

IAM proporciona una variedad de funciones para que usted pueda asegurar el acceso a sus recursos.

## Gestión de permisos refinados

Puede conceder a los usuarios de IAM permisos para gestionar diferentes recursos en su cuenta. Como se muestra en la siguiente figura, puede conceder permiso a Charlie para gestionar recursos de Virtual Private Cloud (VPC) en el proyecto B, y solo conceder permiso a James para ver recursos de VPC en el proyecto B.

**Figura 4-1** Modelo de gestión de permisos




## Acceso seguro

En lugar de compartir su contraseña con otras personas, puede crear usuarios de IAM para empleados o aplicaciones de su organización y generar credenciales de identidad para que puedan acceder de forma segura a recursos específicos según los permisos asignados.

## Protección de operaciones críticas

IAM proporciona protección de inicio de sesión y protección de operaciones críticas, lo que hace que su cuenta y sus recursos sean más seguros. Cuando usted o los usuarios creados con

su cuenta inician sesión en la consola o realizan una operación crítica, usted y los usuarios deben completar la autenticación por correo electrónico, SMS o dispositivo MFA virtual.

## Asignación de permisos basados en grupo de usuarios

Con IAM, no es necesario asignar permisos a usuarios individuales. En su lugar, puede gestionar usuarios por grupo y asignar permisos al grupo especificado. A continuación, cada usuario hereda los permisos de sus grupos. Para cambiar los permisos de un usuario, puede quitarlo de los grupos originales o agregarlo a otros grupos.

## Aislamiento de recursos basado en proyectos

Puede crear subproyectos en una región para que los recursos de esa región puedan aislarse entre sí.

## Autenticación de identidad federada

Las empresas con sistemas de autenticación de identidad pueden acceder a Huawei Cloud a través del inicio de sesión único (SSO), eliminando la necesidad de crear usuarios en Huawei Cloud.

## Delegación de gestión de recursos

Puede delegar cuentas más profesionales y eficientes u otros servicios en la nube para gestionar recursos específicos en su cuenta.

## Ajustes de seguridad de la cuenta

Las políticas de autenticación y contraseñas de inicio de sesión y la lista de control de acceso (ACL) mejoran la seguridad de la información del usuario y los datos del sistema.

## Coherencia eventual

Los resultados de sus operaciones de IAM, como la creación de usuarios y grupos de usuarios y la asignación de permisos, pueden no tener efecto inmediatamente porque los datos se replican en diferentes servidores en los centros de datos de Huawei Cloud en todo el mundo. Asegúrese de que los resultados de la operación hayan surtido efecto antes de realizar cualquier otra operación que dependa de ellos.

# 5 Servicios en la nube compatibles

IAM proporciona autenticación de identidad y gestión de permisos para otros servicios de Huawei Cloud. Los usuarios creados en IAM pueden acceder a estos servicios según los permisos asignados. Para ver todos los permisos de los servicios admitidos por IAM, consulte **Permisos definidos por el sistema**. Para los servicios que no son compatibles con IAM, solo puede usar su cuenta para acceder a estos servicios.

A continuación se enumeran los servicios compatibles con IAM y las descripciones de encabezados de tabla.

- Servicio: Nombre de un servicio en la nube que admite la gestión de permisos mediante IAM.
- Ámbito: la región donde se pueden asignar permisos de acceso para un servicio mediante IAM.
  - Regiones globales: Los servicios desplegados sin especificar regiones físicas se denominan servicios globales. Los permisos para estos servicios deben asignarse en regiones globales. Los usuarios no necesitan cambiar de región cuando acceden a estos servicios.
  - Regiones específicas: Los servicios desplegados para regiones específicas se denominan servicios a nivel de proyecto. Los permisos para estos servicios deben asignarse en regiones específicas y tener efecto solo para las regiones correspondientes. Los usuarios deben cambiar a una de estas regiones cuando acceden a los servicios.
- Consola: si un servicio admite la gestión de permisos mediante la consola IAM.
- API: si un servicio admite la gestión de permisos mediante API.
- Delegación: si se puede delegar un servicio para acceder y gestionar otros servicios en la nube en su nombre.
- Política: si un servicio admite la gestión de permisos basada en políticas. Una política es un conjunto de permisos que definen las operaciones que se pueden realizar en recursos específicos de la nube.
- Proyecto empresarial: Si un servicio apoya la autorización por proyecto empresarial. Para obtener más información acerca de los proyectos de empresa, consulte **Guía de usuario de Enterprise Management**.

NOTA

√: soportado; x: no soportado

## Cómputo

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Elastic Cloud Server (ECS) | Regiones específicas | √ | √ | √ | √ | √ |
| Bare Metal Server (BMS) | Regiones específicas | √ | √ | √ | √ | √ |
| Auto Scaling (AS) | Regiones específicas | √ | √ | x | √ | √ |
| Cloud Phone Host (CPH) | Regiones específicas | √ | √ | x | x | x |
| Image Management Service (IMS) | Regiones específicas | √ | √ | √ | √ | √ |
| FunctionGraph | Regiones específicas | √ | √ | √ | x | √ |
| Dedicated Host (DeH) | Regiones específicas | √ | x | x | √ | √ |

## Almacenamiento

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Elastic Volume Service (EVS) | Regiones específicas | √ | √ | x | √ | √ |
| Storage Disaster Recovery Service (SDRS) | Regiones específicas | √ | √ | x | x | x |
| Cloud Server Backup Service (CSBS) | Regiones específicas | √ | √ | x | x | x |
| Volume Backup Service (VBS) | Regiones específicas | √ | √ | x | x | x |
| Object Storage Service (OBS) | Regiones globales | √ | √ | √ | √ | √ |
| Scalable File Service (SFS) | Regiones específicas | √ | √ | x | √ | √ |

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Content Delivery Network (CDN) | Regiones globales | √ | √ | x | √ | √ |
| Cloud Backup and Recovery (CBR) | Regiones específicas | √ | √ | x | √ | √ |

## Red

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Virtual Private Cloud (VPC) | Regiones específicas | √ | √ | x | √ | √ |
| Elastic Load Balance (ELB) | Regiones específicas | √ | √ | x | √ | √ |
| Domain Name Service (DNS) | Regiones globales | √ | √ | x | x | √ |
| NAT Gateway | Regiones específicas | √ | √ | x | √ | √ |
| Direct Connect | Regiones específicas | √ | x | x | x | x |
| Virtual Private Network (VPN) | Regiones específicas | √ | x | x | √ | x |
| Cloud Connect (CC) | Regiones específicas | √ | x | x | √ | √ |
| VPC Endpoint (VPCEP) | Regiones específicas | √ | √ | x | x | x |

## Contenedores

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Cloud Container Engine (CCE) | Regiones específicas | √ | √ | x | √ | √ |

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Cloud Container Instance (CCI) | Regiones específicas | √ | √ | x | √ | √ |
| Software Repository for Container (SWR) | Regiones específicas | √ | √ | x | √ | x |
| Gene Container Service (GCS) | Regiones específicas | √ | √ | x | √ | √ |

## Base de datos

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Relational Database Service (RDS) | Regiones específicas | √ | √ | x | √ | √ |
| Document Database Service (DDS) | Regiones específicas | √ | x | x | √ | √ |
| Distributed Database Middleware (DDM) | Regiones específicas | √ | √ | x | √ | √ |
| Data Replication Service (DRS) | Regiones específicas | √ | √ | x | √ | √ |
| Data Admin Service (DAS) | Regiones específicas | √ | x | x | x | x |
| GaussDB NoSQL | Regiones específicas | √ | √ | x | √ | √ |

## Seguridad & Cumplimiento

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Anti-DDoS | Regiones específicas | √ | √ | x | x | x |

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Advanced Anti-DDoS (AAD) | Regiones específicas | √ | √ | √ | x | √ |
| Cloud Native Anti-DDoS (CNAD) | Regiones globales | √ | √ | x | √ | x |
| Web Application Firewall (WAF) | Regiones específicas | √ | x | x | x | √ |
| Cloud Firewall (CFW) | Regiones específicas | √ | x | x | √ | x |
| Vulnerability Scan Service (VSS) | Regiones específicas | √ | x | x | x | x |
| Host Security Service (HSS) | Regiones específicas | √ | x | x | x | √ |
| Database Security Service (DBSS) | Regiones específicas | √ | x | x | √ | x |
| Data Encryption Workshop (DEW) | Regiones específicas | √ | √ | x | x | x |
| Managed Detection and Response (MDR) | Regiones específicas | √ | x | x | x | x |
| SSL Certificate Manager (SCM) | Regiones globales | √ | √ | x | √ | x |
| Container Guard Service (CGS) | Regiones específicas | √ | x | x | √ | x |
| Situation Awareness (SA) | Regiones globales | √ | √ | √ | √ | x |
| Cloud Bastion Host (CBH) | Regiones específicas | √ | √ | x | √ | x |
| Data Security Center (DSC) | Regiones específicas | √ | √ | x | √ | x |

## Gestión & Gobernanza

| Servicio | Alcance | Consola | API | Delegación | Política de grano fino | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Identity and Access Management (IAM) | Regiones globales | √ | √ | x | √ | x |
| Cloud Eye | Regiones específicas | √ | √ | x | √ | √ |
| Cloud Trace Service (CTS) | Regiones específicas | √ | √ | x | x | x |
| Application Performance Management (APM) | Regiones específicas | √ | √ | x | √ | √ |
| Application Operations Management (AOM) | Regiones específicas | √ | √ | x | √ | √ |
| Log Tank Service (LTS) | Regiones específicas | √ | √ | x | √ | √ |
| Tag Management Service (TMS) | Regiones globales | √ | √ | x | x | x |

## Aplicación

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| ServiceStage | Regiones específicas | √ | √ | x | x | x |
| Distributed Cache Service (DCS) | Regiones específicas | √ | √ | √ | √ | √ |
| Distributed Message Service for Kafka (DMS for Kafka) | Regiones específicas | √ | √ | x | √ | √ |
| Distributed Message Service for RabbitMQ (DMS for RabbitMQ) | Regiones específicas | √ | √ | x | √ | √ |

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Distributed Message Service for RocketMQ (DMS for RocketMQ) | Regiones específicas | √ | √ | x | √ | √ |
| Simple Message Notification (SMN) | Regiones específicas | √ | √ | x | x | √ |
| Cloud Service Engine (CSE) | Regiones específicas | √ | √ | x | x | √ |
| Cloud Performance Test Service (CPTS) | Regiones específicas | √ | √ | x | x | x |
| API Gateway | Regiones específicas | √ | √ | x | x | √ |
| Blockchain Service (BCS) | Regiones específicas | √ | √ | x | √ | √ |

## DeC

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Dedicated Distributed Storage Service (DSS) | Regiones específicas | √ | √ | x | √ | x |

## Migración

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Server Migration Service (SMS) | Regiones globales | √ | x | x | √ | x |
| Object Storage Migration Service (OMS) | Regiones específicas | √ | x | x | x | x |

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Cloud Data Migration (CDM) | Regiones específicas | √ | √ | √ | √ | √ |

## Borde inteligente

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| CloudLake | Regiones globales | √ | x | x | √ | x |

## EI

| Servicio | Alcance | Consola | API | Delegación | Política de grano fino | Proyecto empresarial |
|---|---|---|---|---|---|---|
| ModelArts | Regiones específicas | √ | √ | √ | √ | √ |
| Data Lake Governance Center (DGC) | Regiones específicas | √ | √ | √ | √ | x |
| MapReduce Service (MRS) | Regiones específicas | √ | √ | x | √ | √ |
| Data Warehouse Service (DWS) | Regiones específicas | √ | √ | √ | √ | √ |
| CloudTable | Regiones específicas | √ | √ | x | x | √ |
| Data Lake Insight (DLI) | Regiones específicas | √ | √ | x | x | √ |
| Data Ingestion Service (DIS) | Regiones específicas | √ | √ | √ | x | √ |
| Cloud Search Service (CSS) | Regiones específicas | √ | √ | √ | x | √ |

| Servicio | Alcance | Consola | API | Delegación | Política de grano fino | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Graph Engine Service (GES) | Regiones específicas | √ | √ | √ | x | √ |
| Recommender System (RES) | Regiones específicas | √ | √ | x | √ | √ |
| Content Moderation | Regiones específicas | √ | √ | x | √ | x |
| Conversational Bot Service (CBS) | Regiones específicas | √ | √ | x | x | x |
| Huawei HiLens | Regiones específicas | √ | x | x | √ | x |
| Trusted Intelligent Computing Service (TICS) | Regiones específicas | √ | x | x | √ | x |

## Aplicaciones empresariales

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Workspace | Regiones específicas | √ | √ | x | × | x |
| ROMA Connect | Regiones específicas | √ | √ | √ | √ | √ |
| CloudSite | Regiones específicas | √ | x | √ | √ | x |

## Comunicaciones en la nube

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Voice Call | Regiones específicas | √ | √ | √ | x | x |

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Message & SMS | Regiones específicas | √ | √ | √ | √ | x |
| Private Number | Regiones específicas | √ | √ | √ | √ | x |

## Vídeo

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Media Processing Center (MPC) | Regiones específicas | √ | √ | √ | x | x |
| Video on Demand (VOD) | Regiones específicas | √ | √ | √ | √ | x |

## Desarrollo y O&M

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| CodeArts | Regiones específicas | √ | x | x | √ | √ |
| CodeArts Req | Regiones específicas | √ | √ | x | √ | x |
| CloudIDE | Regiones específicas | √ | √ | x | √ | x |

## Soporte para el usuario

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| My Account | Regiones específicas | √ | x | x | √ | x |
| Billing Center | Regiones específicas | √ | x | x | √ | x |
| Resource Center | Regiones específicas | √ | x | x | √ | x |
| **Enterprise Project Management Service (EPS)** | Regiones globales | √ | √ | x | √ | x |
| **Service Tickets** | Regiones globales | √ | √ | x | x | x |
| ICP License Service | Regiones globales | √ | x | x | x | x |
| Professional Services | Regiones globales | √ | x | x | √ | x |

## Otros

| Servicio | Alcance | Consola | API | Delegación | Política | Proyecto empresarial |
|---|---|---|---|---|---|---|
| Message Center | Regiones específicas | √ | x | x | √ | x |

# 6 Permisos

Si necesita asignar diferentes permisos para IAM a los empleados de su organización, IAM es una buena opción para la gestión de permisos detallada. IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a proteger el acceso a sus recursos de Huawei Cloud.

Con IAM, puede crear usuarios de IAM bajo su cuenta y asignar permisos a estos usuarios para controlar su acceso a recursos específicos. Por ejemplo, puede conceder permisos para permitir que determinados planificadores de proyectos de su empresa vean los datos de IAM, pero no permitirles realizar operaciones de alto riesgo, por ejemplo, eliminar usuarios y proyectos de IAM. Para ver todos los permisos de los servicios admitidos por IAM, consulte **Permisos definidos por el sistema**.

## Permisos de IAM

Los nuevos usuarios de IAM no tienen ningún permiso asignado de forma predeterminada. Primero debe agregarlos a uno o más grupos y adjuntar políticas o roles a estos grupos. A continuación, los usuarios heredan los permisos de los grupos y pueden realizar operaciones específicas en servicios en la nube en función de los permisos que se les han asignado.

IAM es un servicio global desplegado para todas las regiones. Cuando establece el ámbito de autorización en **Global services**, los usuarios tienen permiso para acceder a IAM en todas las regiones.

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Una estrategia de autorización de grano grueso proporcionada por IAM para asignar permisos en función de las responsabilidades del trabajo de los usuarios. Solo un número limitado de roles de nivel de servicio están disponibles para autorización. Los servicios en la nube dependen unos de otros. Cuando concede permisos mediante roles, también debe adjuntar las dependencias de roles existentes. Los roles no son ideales para la autorización detallada y el acceso con privilegios mínimos.
- Políticas: Una estrategia de autorización detallada que define los permisos necesarios para realizar operaciones en recursos específicos en la nube bajo ciertas condiciones. Este tipo de autorización es más flexible y es ideal para el acceso de privilegios mínimos. Por ejemplo, puede conceder a los usuarios solo permiso para gestionar ECS de un tipo determinado. La mayoría de las políticas detalladas contienen permisos para API específicas, y los permisos se definen mediante acciones de API. Para ver las acciones de API admitidas por IAM, consulte **Permisos y acciones admitidas**.

**Tabla 6-1** enumera todos los permisos definidos por el sistema para IAM.

**Tabla 6-1** Permisos definidos por el sistema para IAM

| Nombre de rol/ política | Descripción | Tipo | Contenido |
|---|---|---|---|
| FullAccess | Permisos completos para todos los servicios que admiten la autorización basada en políticas. Los usuarios con estos permisos pueden realizar operaciones en todos los servicios. | Política definida por el sistema | **Contenido de la Política FullAccess** |
| IAM ReadOnlyAccess | Permisos de sólo lectura para IAM. Los usuarios con estos permisos solo pueden ver los datos de IAM. | Política definida por el sistema | **Contenido de la Política de ReadOnlyAccess de IAM** |
| Security Administrator | Administrador de IAM con permisos completos, incluidos permisos para crear y eliminar usuarios de IAM. | Rol definido por el sistema | **Contenido del rol de administrador de seguridad** |
| Agent Operator | Operador IAM (parte delegada) con permisos para cambiar roles y acceder a recursos de una parte delegada. | Rol definido por el sistema | **Contenido del rol de operador de agente** |
| Tenant Guest | Permisos de sólo lectura para todos los servicios excepto IAM. | Política definida por el sistema | **Contenido del rol de invitado del tenant** |
| Tenant Administrator | Permisos de administrador para todos los servicios excepto IAM. | Política definida por el sistema | **Contenido del rol de Administrador del tenant** |

**Tabla 6-2** enumera las operaciones comunes admitidas por los permisos definidos por el sistema para IAM.

NOTA

**Tenant Guest** y **Tenant Administrator** son roles básicos proporcionados por IAM y no contienen ningún permiso específico para IAM. Por lo tanto, los dos roles no se enumeran en la tabla siguiente.

**Tabla 6-2** Operaciones comunes admitidas por permisos definidos por el sistema

| Operación | Administrador de seguridad | Agente Operador | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Creación de usuarios de IAM | Admitido | No admitido | Admitido | No admitido |
| Consulta de los detalles del usuario de IAM | Admitido | No admitido | Admitido | Admitido |
| Modificación de la información de usuario de IAM | Admitido | No admitido | Admitido | No admitido |
| Consulta de la configuración de seguridad de los usuarios de IAM | Admitido | No admitido | Admitido | Admitido |
| Modificación de la configuración de seguridad de los usuarios de IAM | Admitido | No admitido | Admitido | No admitido |
| Eliminación de usuarios de IAM | Admitido | No admitido | Admitido | No admitido |
| Creación de grupos de usuarios | Admitido | No admitido | Admitido | No admitido |
| Consulta de detalles del grupo de usuarios | Admitido | No admitido | Admitido | Admitido |
| Modificación de la información del grupo de usuarios | Admitido | No admitido | Admitido | No admitido |

| Operación | Administrador de seguridad | Agente Operador | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Adición de usuarios a grupos de usuarios. | Admitido | No admitido | Admitido | No admitido |
| Eliminación de usuarios de grupos de usuarios | Admitido | No admitido | Admitido | No admitido |
| Eliminación de grupos de usuarios | Admitido | No admitido | Admitido | No admitido |
| Asignación de permisos a grupos de usuarios | Admitido | No admitido | Admitido | No admitido |
| Eliminación de permisos de grupos de usuarios | Admitido | No admitido | Admitido | No admitido |
| Creación de políticas personalizadas | Admitido | No admitido | Admitido | No admitido |
| Modificación de políticas personalizadas | Admitido | No admitido | Admitido | No admitido |
| Eliminación de políticas personalizadas | Admitido | No admitido | Admitido | No admitido |
| Consulta de detalles de permisos | Admitido | No admitido | Admitido | Admitido |
| Creación de delegaciones | Admitido | No admitido | Admitido | No admitido |
| Consulta de delegaciones | Admitido | No admitido | Admitido | Admitido |
| Modificación de delegaciones | Admitido | No admitido | Admitido | No admitido |
| Cambio de roles | No admitido | Admitido | Admitido | No admitido |

| Operación | Administrador de seguridad | Agente Operador | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Eliminación de delegaciones | Admitido | No admitido | Admitido | No admitido |
| Concesión de permisos a delegaciones | Admitido | No admitido | Admitido | No admitido |
| Eliminación de permisos de delegaciones | Admitido | No admitido | Admitido | No admitido |
| Creación de proyectos | Admitido | No admitido | Admitido | No admitido |
| Consulta de proyectos | Admitido | No admitido | Admitido | Admitido |
| Modificación de proyectos | Admitido | No admitido | Admitido | No admitido |
| Supresión de proyectos | Admitido | No admitido | Admitido | No admitido |
| Creación de proveedores de identidad | Admitido | No admitido | Admitido | No admitido |
| Importación de archivos de metadatos | Admitido | No admitido | Admitido | No admitido |
| Consulta de archivos de metadatos | Admitido | No admitido | Admitido | Admitido |
| Consulta de proveedores de identidad | Admitido | No admitido | Admitido | Admitido |
| Consulta de protocolos | Admitido | No admitido | Admitido | Admitido |
| Consulta de asignaciones | Admitido | No admitido | Admitido | Admitido |
| Actualización de proveedores de identidad | Admitido | No admitido | Admitido | No admitido |
| Actualización de protocolos | Admitido | No admitido | Admitido | No admitido |

| Operación | Administrador de seguridad | Agente Operador | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Actualización de asignaciones | Admitido | No admitido | Admitido | No admitido |
| Supresión de proveedores de identidad | Admitido | No admitido | Admitido | No admitido |
| Supresión de protocolos | Admitido | No admitido | Admitido | No admitido |
| Supresión de asignaciones | Admitido | No admitido | Admitido | No admitido |
| Consulta de cuotas | Admitido | No admitido | Admitido | No admitido |

La gestión de claves de acceso está deshabilitada de forma predeterminada. Cuando se habilita **la gestión de claves de acceso**, solo los administradores pueden gestionar las claves de acceso. Si los usuarios de IAM necesitan crear, habilitar, deshabilitar o eliminar sus propias claves de acceso, deben pedir al administrador que **deshabilite la gestión de claves de acceso**.

Si un usuario de IAM desea gestionar las claves de acceso de otros usuarios de IAM, consulte la **Tabla 3**. Por ejemplo, si el usuario A de IAM desea crear una clave de acceso para el usuario B de IAM, el usuario A de IAM debe tener el permiso de Administrador de seguridad o FullAccess.

**Tabla 6-3** Acceder a las operaciones clave admitidas por las políticas o roles definidos por el sistema

| Operación | Administrador de seguridad | Agente Operador | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Creación de claves de acceso (para otros usuarios de IAM) | Admitido | No admitido | Admitido | No admitido |
| Consulta de claves de acceso (de otros usuarios de IAM) | Admitido | No admitido | Admitido | Admitido |

| Operación | Administrador de seguridad | Agente Operador | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Modificación de claves de acceso (para otros usuarios de IAM) | Admitido | No admitido | Admitido | No admitido |
| Eliminación de claves de acceso (para otros usuarios de IAM) | Admitido | No admitido | Admitido | No admitido |

## Contenido de la Política FullAccess

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

## Contenido de la Política de ReadOnlyAccess de IAM

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

## Contenido del rol de administrador de seguridad

```
{
    "Version": "1.0",
    "Statement": [
        {
            "Action": [
                "iam:agencies:*",
                "iam:credentials:*",
                "iam:groups:*",
                "iam:identityProviders:*",
                "iam:mfa:*",
                "iam:permissions:*",
                "iam:projects:*",
                "iam:quotas:*",
```

```
                "iam:roles:*",
                "iam:users:*",
                "iam:securitypolicies:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

## Contenido del rol de operador de agente

```
{
    "Version": "1.0",
    "Statement": [
        {
            "Action": [
                "iam:tokens:assume"
            ],
            "Effect": "Allow"
        }
    ]
}
```

## Contenido del rol de invitado del tenant

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

## Contenido del rol de Administrador del tenant

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

```
                    "g:ServiceName": [
                        "iam"
                    ]
                }
            },
            "Action": [
                "*:*:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

# 7 Seguridad



## 7.1 Responsabilidades compartidas

Huawei garantiza que su compromiso con la seguridad cibernética nunca se verá compensado por la consideración de intereses comerciales. Para hacer frente a los desafíos emergentes de seguridad en la nube y a las amenazas y ataques generalizados de seguridad en la nube, Huawei Cloud crea un sistema integral de garantía de seguridad de servicios en la nube para diferentes regiones e industrias basado en las ventajas únicas de software y hardware, las leyes, las regulaciones, los estándares de la industria y el ecosistema de seguridad de Huawei.

**Figura 7-1** ilustra las responsabilidades compartidas por Huawei Cloud y los usuarios.

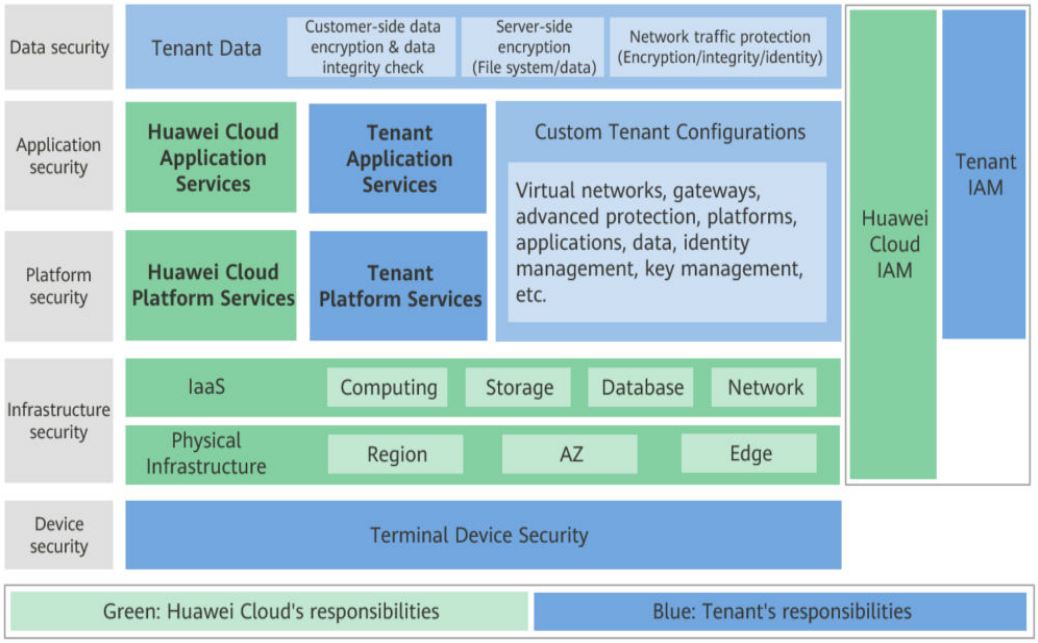
- **Huawei Cloud**: Garantizar la seguridad de los servicios en la nube y proporcionar nubes seguras. Las responsabilidades de seguridad de Huawei Cloud incluyen garantizar la seguridad de nuestros servicios IaaS, PaaS y SaaS, así como los entornos físicos de los centros de datos de Huawei Cloud donde nuestros IaaS, PaaS, y los servicios SaaS operan. Huawei Cloud es responsable no solo de las funciones de seguridad y el rendimiento de nuestra infraestructura, servicios en la nube y tecnologías, sino también de la seguridad general de la nube y, en el sentido más amplio, del cumplimiento de seguridad de nuestra infraestructura y servicios.
- **Tenant**: Utilizar la nube de forma segura. Los inquilinos de Huawei Cloud son responsables de la gestión segura y efectiva de las configuraciones personalizadas por el inquilino de los servicios en la nube, incluidos IaaS, PaaS y SaaS. Esto incluye, entre otros, redes virtuales, el sistema operativo de los hosts e invitados de máquinas virtuales, firewalls virtuales, API Gateway, servicios de seguridad avanzados, todo tipo de servicios en la nube, datos del inquilino, cuentas de identidad, y gestión de claves.

**Libro blanco de seguridad de Huawei Cloud** elabora las ideas y medidas para construir la seguridad en Huawei Cloud, incluidas las estrategias de seguridad en la nube, el modelo de

responsabilidad compartida, el cumplimiento y la privacidad, las organizaciones y el personal de seguridad, la seguridad de la infraestructura, el servicio y la seguridad del inquilino, la seguridad de ingeniería, seguridad de O&M y seguridad del ecosistema.

**Figura 7-1** Modelo de responsabilidad de seguridad compartida de Huawei Cloud




# 7.2 Control de acceso y autenticación

## 7.2.1 Autenticación de identidad

El servicio IAM requiere que el solicitante de acceso presente la credencial de identidad y verifique la validez de identidad. Además, el servicio IAM proporciona protección de inicio de sesión y políticas de verificación para reforzar la seguridad de la autenticación de identidad.

### Credenciales de identidad y su seguridad

Se puede acceder a IAM mediante cuentas y usuarios de IAM. Ambos soportan la autenticación de identidad usando nombres de usuario, contraseñas, claves de acceso y claves de acceso temporales. IAM implementa el diseño de seguridad para cada credencial de identidad para proteger los datos de los usuarios y permitir que los usuarios accedan a IAM de forma más segura. Para obtener más información, véase **Tabla 7-1**.

**Tabla 7-1** Credenciales de identidad de IAM y diseño de seguridad

| Credencial de acceso | Descripción de seguridad | Referencia |
| --- | --- | --- |
| Nombre de usuario y contraseña | Puede configurar el tipo de carácter y la longitud mínima de una clave de usuario según sea necesario. También puede configurar la política de período de validez de contraseña y la política de período de validez mínimo de contraseña. | **Política de contraseña** |
| Clave de acceso | AK se utiliza junto con SK para firmar solicitudes criptográficamente, asegurando que las solicitudes sean secretas, completas y correctas. | **Claves de acceso** |
| Clave de acceso temporal | Además de la función de clave de acceso, una clave de acceso temporal tiene un período de validez que se puede personalizar. Si el período de validez expira, la clave de acceso temporal no será válida y deberá obtener una nueva. | **Clave de acceso temporal (para usuarios federados)** |

## Políticas de autenticación y protección de inicio de sesión

Como se describe en el documento **Tabla 7-2**, además de requerir que los usuarios muestren credenciales y verifiquen su validez durante el inicio de sesión, IAM también proporciona protección de inicio de sesión y admite políticas de verificación de inicio de sesión para evitar que la información del usuario sea robada.

**Tabla 7-2** Políticas de autenticación y protección de inicio de sesión

| Método de protección de inicio de sesión | Descripción | Funciones |
| --- | --- | --- |
| Protección de inicio de sesión | Además de introducir el nombre de usuario y la contraseña en la página de inicio de sesión (autenticación por primera vez), debe introducir un código de verificación en la página **Login Verification** (autenticación por segunda vez).<br>Verifique que los números móviles, las direcciones de correo electrónico y los dispositivos MFA virtuales sean compatibles. Para obtener más información, consulte **Autenticación de MFA**. | **Protección de inicio de sesión** |
| Política de autenticación de inicio de sesión | IAM admite las siguientes políticas de autenticación de inicio de sesión:<br>Política de **tiempo de espera de la sesión**: Si un usuario no inicia sesión en el sistema dentro de un período especificado, el usuario debe iniciar sesión de nuevo.<br>Política de **bloqueo de cuenta**: Si el número de errores de inicio de sesión excede el umbral, la cuenta está bloqueada.<br>Política de **desactivación de cuenta**: Si un usuario no inicia sesión en el sistema durante mucho tiempo, la cuenta está deshabilitada.<br>Visualización de **información de inicio de sesión reciente**: Permite a los usuarios ver la última hora de inicio de sesión. | **Política de autenticación de inicio de sesión** |

### 7.2.2 Configuración del control de acceso

IAM utiliza políticas de autorización y ACL de grano fino para controlar el acceso.

**Tabla 7-3** Control de acceso IAM

| Política de acceso | Descripción | Referencia |
| --- | --- | --- |
| Política de autorización detallada de IAM | Los permisos de servicio de IAM se dividen en roles o políticas detalladas. Los roles y las políticas definen las operaciones de usuario permitidas o rechazadas por IAM. Por ejemplo, si un usuario o grupo de usuarios tiene el permiso ReadOnlyAccess de IAM, el usuario o grupo de usuarios solo tiene el permiso de solo lectura en los datos de servicio de IAM. IAM también admite **políticas personalizadas** para asignar permisos de servicio de IAM. | **Permisos de IAM** |
| ACL | Con ACL, puede establecer políticas de control de acceso para permitir a los usuarios iniciar sesión en la consola de IAM o abrir API solo desde intervalos de direcciones IP, segmentos de red y puntos de conexión de VPC especificados. | **ACL** |

## 7.3 Protección de datos

### 7.3.1 El lado de IAM

Para garantizar que sus datos personales, como el nombre de usuario, la contraseña y el número de teléfono móvil, no sean obtenidos por entidades o personas no autorizadas o no autenticadas, IAM cifra sus datos durante el almacenamiento y la transmisión para evitar la fuga de datos.

#### Datos personales

**Tabla 7-4** enumera los datos personales generados o recopilados por IAM.

**Tabla 7-4** Datos personales

| Tipo | Origen | Utilizado para | Modificable | Obligatorio |
|---|---|---|---|---|
| Nombre de usuario. | ● Se introduce cuando se crea un usuario en la consola de gestión.<br>● Se introduce cuando se invoca a una API. | ● Identificación de la identidad del usuario<br>● Autenticación de identidad durante el acceso a la consola o la invocación a la API | Sí (los administradores pueden invocar a la API para cambiar el nombre de usuario) | Sí<br>Los nombres de usuario se utilizan para identificar a los usuarios. |
| Contraseña | ● Se especifica cuando se crea un usuario, se modifican las credenciales de usuario o se restablece la contraseña en la consola de gestión.<br>● Se introduce cuando se invoca a una API. | Autenticación de identidad durante el acceso a la consola o la invocación a la API | Sí | No<br>También puede elegir la autenticación AK/SK. |
| Dirección de correo electrónico | Se introduce cuando se crea un usuario, se modifican las credenciales de usuario o se cambia la dirección de correo electrónico en la consola de gestión. | ● Identificación de la identidad del usuario<br>● Autenticación de identidad durante el acceso a la consola<br>● Recibir mensajes | Sí | No |

| Tipo | Origen | Utilizado para | Modificable | Obligatorio |
|---|---|---|---|---|
| Número de celular | Se introduce cuando se crea un usuario, se modifican las credenciales de usuario o se cambia el número de teléfono móvil en la consola de gestión. | • Identificación de la identidad del usuario<br>• Autenticación de identidad durante el acceso a la consola<br>• Recibir mensajes | Sí | No |
| AK/SK | Se muestra en el área **Security Settings** > **Access Keys** de un usuario específico en la consola de IAM o en la página **My Credentials** > **Access Keys**. | Autenticación de identidad durante la invocación a la API | No<br>AK/SK no se puede modificar, pero se pueden eliminar y crear de nuevo. | No<br>AK/SK se utilizan para firmar las solicitudes enviadas a las API de invocación. |

### Seguridad de almacenamiento de datos

IAM utiliza algoritmos de encriptación para cifrar los datos de usuario antes de almacenarlos.

- Nombres de usuario y AK: datos no confidenciales, que se almacenan en texto plano.
- Contraseña: la contraseña se cifra mediante el algoritmo SHA512 salado.
- Dirección de correo electrónico, número de teléfono móvil y SK: Utilice el algoritmo AES para cifrarlos y almacenarlos.

### Seguridad de transmisión de datos

Los datos confidenciales (incluidas las contraseñas) de los usuarios se cifran utilizando TLS 1.2 durante la transmisión. Todas las API de IAM admiten HTTPS para cifrar datos durante la transmisión.

## 7.3.2 El lado del tenant

**Responsabilidades compartidas** se aplican a la protección de datos en Huawei Cloud IAM. Como se mencionó anteriormente, IAM es responsable de la seguridad del servicio en sí y proporciona un mecanismo de protección de datos seguro. Los tenants son responsables del uso seguro de los servicios de IAM, incluida la configuración de parámetros de seguridad y la separación y concesión de permisos por parte de las empresas.

A los efectos de la protección de datos, se le aconseja que utilice IAM de una manera más estándar haciendo referencia a **Recomendaciones para el uso de IAM**.

# 7.4 Resiliencia

Los centros de datos de Huawei Cloud se despliegan en todo el mundo. Todos los centros de datos están funcionando correctamente. Los centros de datos en dos ciudades se despliegan como centro de recuperación ante desastres uno para el otro. Si un centro de datos en la ciudad A está inactivo, el centro de datos en la ciudad B se hace cargo automáticamente del trabajo y sirve sus aplicaciones y datos de acuerdo con las regulaciones para garantizar la continuidad del servicio. Con el fin de minimizar las interrupciones del servicio causadas por fallas de hardware, desastres naturales u otros eventos desastrosos, Huawei Cloud ofrece un plan de recuperación ante desastres para todos los centros de datos:

Como servicio básico de autenticación de identidad, Huawei Cloud IAM se ha desplegado en varias zonas para proporcionar a los usuarios globales una mayor disponibilidad, tolerancia a fallos y escalabilidad.

# 7.5 Auditoría y monitoreo

Cloud Trace Service (CTS) registra las operaciones realizadas en los recursos de la nube en su cuenta. Los registros de operaciones se pueden utilizar para realizar análisis de seguridad, realizar un seguimiento de los cambios de recursos, realizar auditorías de cumplimiento y localizar fallos.

Para obtener detalles sobre las operaciones de IAM que pueden grabarse por CTS, consulte "Operaciones de IAM que pueden grabarse por CTS" en **Habilitación de CTS**. Después de habilitar CTS y crear y configurar un rastreador, CTS comienza a registrar las operaciones para la auditoría. Para obtener más información, consulte **Habilitación de CTS**. Después de habilitar CTS, puede **ver los registros de auditoría de IAM**. CTS almacena los registros de operaciones de los últimos siete días.

CTS le permite **configurar notificaciones de eventos clave**. Puede agregar operaciones sensibles y de alto riesgo relacionadas con IAM como operaciones clave a la lista de monitoreo en tiempo real de CTS para monitoreo y rastreo. Si se activa una operación clave en la lista de monitoreo cuando un usuario utiliza el servicio IAM, CTS registra el registro de operaciones y envía una notificación al abonado relacionado en tiempo real.

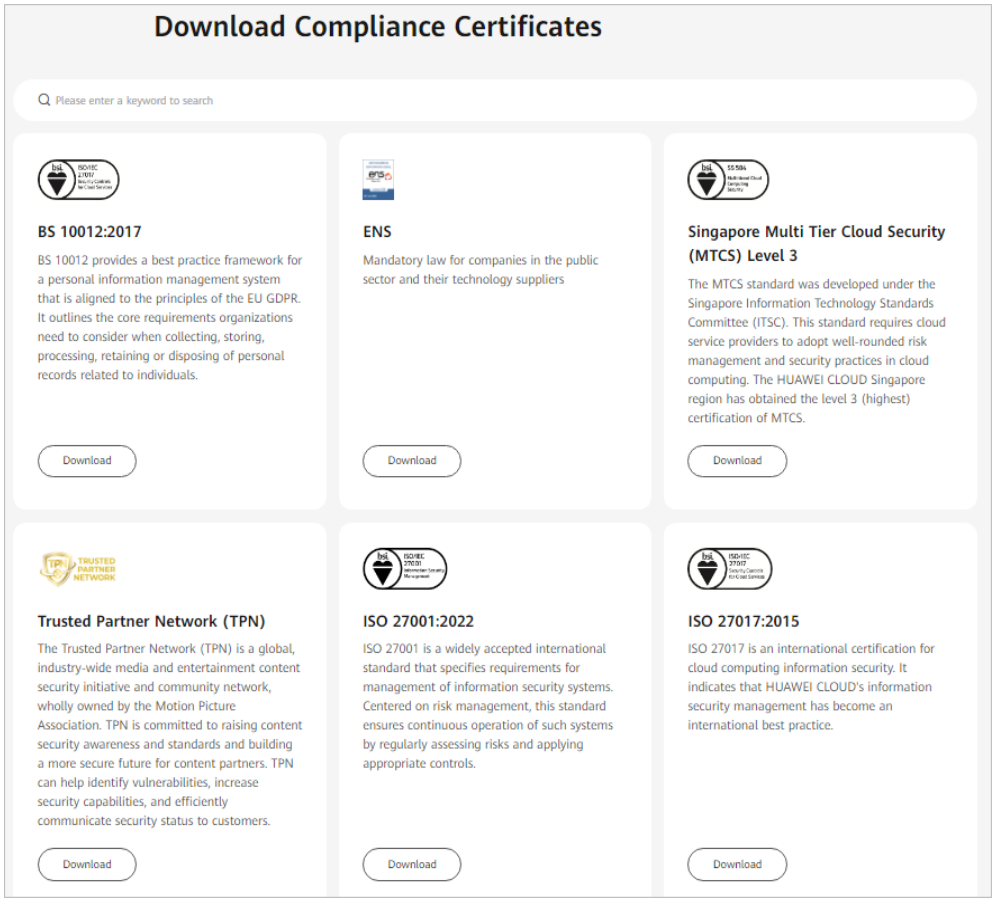
# 7.6 Certificados

## Certificados de Cumplimiento

Los servicios y plataformas de Huawei Cloud han obtenido diversas certificaciones de seguridad y cumplimiento de organizaciones autorizadas, como la Organización Internacional de Normalización (ISO). Puede **descargarlos** desde la consola.

**Figura 7-2** Descarga de certificados de cumplimiento

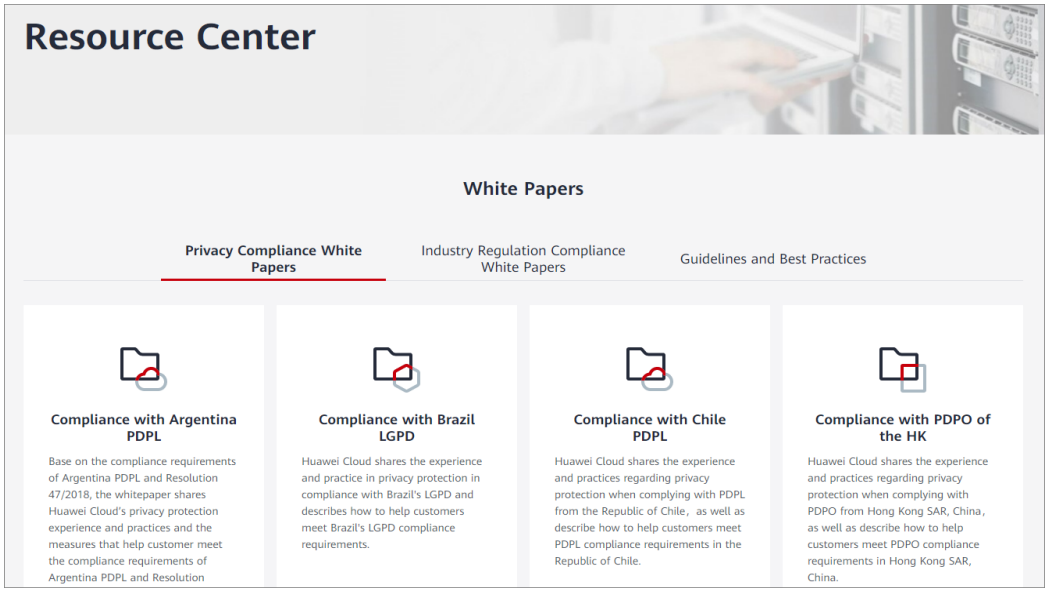



## Centro de recursos

Huawei Cloud también proporciona los siguientes recursos para ayudar a los usuarios a cumplir con los requisitos de cumplimiento. Para obtener más información, consulte **Centro de recursos**.

**Figura 7-3** Centro de recursos



# 8 Notas y restricciones

En la siguiente tabla se enumeran las cuotas de varios recursos en IAM. Para obtener más información, consulte **¿Cómo puedo aumentar mi cuota?**

| Categoría | Concepto | Cuota | Ajustable |
|---|---|---|---|
| Usuario | Usuarios de IAM | 50 | Sí |
| | Caracteres permitidos en un nombre de usuario | 32 | No |
| | Grupos a los que se puede agregar un usuario | 10 | No |
| | Pares AK/SK que un usuario puede crear | 2 | No |
| | Dispositivos MFA virtuales que pueden asociarse con un usuario | 1 | No |
| | Permisos (incluidos los permisos definidos por el sistema y las políticas personalizadas) que se pueden asignar a un usuario para proyectos de empresa | 500 | Sí |
| Grupo de usuario | Grupos de usuarios | 20 | Sí |

| Categoría | Concepto | Cuota | Ajustable |
| --- | --- | --- | --- |
| | Caracteres permitidos en un nombre de grupo de usuarios | 64 | No |
| | Usuarios que se pueden agregar a un grupo de usuarios | Usuarios de IAM que han sido creados con su cuenta | No |
| | Permisos (incluidos los permisos definidos por el sistema y las políticas personalizadas) que se pueden asignar a un grupo de usuarios para proyectos de IAM | 200 | Sí |
| | Permisos (incluidos los permisos definidos por el sistema y las políticas personalizadas) que se pueden asignar a un grupo de usuarios para proyectos de empresa | 500 | Sí |
| Proyecto | Subproyectos en cada región | 10 | Yes |
| Política | Caracteres permitidos en un nombre de política | 64 | No |
| Política personalizada | Políticas personalizadas | 200 | Sí |
| | Caracteres por política | 6,144 | No |
| | Sentencia por política | Ilimitado | No |
| | Acciones por sentencia | Ilimitado | No |
| | Recursos por sentencia | Ilimitado | No |

| Categoría | Concepto | Cuota | Ajustable |
|---|---|---|---|
| | Condiciones por sentencia | Ilimitado | No |
| Delegación | Delegaciones | 50 | Sí |
| | Caracteres permitidos en el nombre de una delegación | 64 | No |
| | Permisos (incluidos los permisos definidos por el sistema y las políticas personalizadas) que se pueden asignar a una delegación | 200 | Sí |
| Proveedor de identidades | Cantidad | 10 | Sí |
| | Caracteres que pueden estar contenidos en un nombre de proveedor de identidad | 64 | No |
| | Reglas de asignación de todos los proveedores de identidad de una cuenta | 10 | Sí |

# 9 Historial de cambio

**Tabla 9-1** Historial de cambio

| Fecha | Descripción |
| --- | --- |
| 2022-11-10 | Esta edición es el decimoctavo lanzamiento oficial, que incorpora el siguiente cambio:<br>Agregada una introducción a las características de seguridad de IAM de **7 Seguridad**. |
| 2021-12-01 | Esta versión es el decimoséptimo lanzamiento oficial, que incorpora el siguiente cambio:<br>Añadida la cuota de regla de conversión de identidad de **8 Notas y restricciones**. |
| 2021-11-23 | Esta edición es la decimosexta versión oficial, que incorpora el siguiente cambio:<br>Agregada la descripción de los proyectos de empresa de **5 Servicios en la nube compatibles**. |
| 2021-04-25 | Esta versión es el decimoquinto lanzamiento oficial, que incorpora el siguiente cambio:<br>Añadidas cuotas de permisos en **8 Notas y restricciones**. |
| 2020-12-30 | Esta edición es la decimocuarta versión oficial, que incorpora el siguiente cambio:<br>Actualizadas las capturas de pantalla de **3 Conceptos básicos** según el cambio en el método de inicio de sesión. |
| 2020-11-30 | Esta edición es la decimotercera versión oficial, que incorpora el siguiente cambio:<br>Actualizada la descripción basada en los cambios en la página de configuración de seguridad. |
| 2020-10-27 | Esta versión es la duodécima versión oficial, que incorpora el siguiente cambio:<br>Actualizadas las capturas de pantalla de **3 Conceptos básicos** según el cambio en el método de inicio de sesión. |

| Fecha | Descripción |
| --- | --- |
| 2020-09-30 | Esta edición es la undécima versión oficial, que incorpora el siguiente cambio:<br>Agregada la sección **6 Permisos**. |
| 2020-06-11 | Esta edición es el décimo lanzamiento oficial, que incorpora el siguiente cambio:<br>Cambiado el número máximo de grupos de usuarios a los que se puede agregar un usuario a **10** en **8 Notas y restricciones**. |
| 2020-06-08 | Esta edición es la novena versión oficial, que incorpora el siguiente cambio:<br>Agregadas descripciones sobre el ID de HUAWEI en **3 Conceptos básicos** y actualizadas las capturas de pantalla de la página de inicio de sesión. |
| 2020-01-19 | Esta versión es el octavo lanzamiento oficial, que incorpora los siguientes cambios:<br>● Optimizado la descripción de los permisos de **3 Conceptos básicos**.<br>● Agregado el límite de subproyectos en una región de **8 Notas y restricciones**. |
| 2019-11-20 | Esta edición es el séptimo lanzamiento oficial, que incorpora el siguiente cambio:<br>Aumentado la cuota de política personalizada a 200 en **8 Notas y restricciones**. |
| 2019-06-05 | Esta edición es el sexto lanzamiento oficial.<br>Descripciones modificadas en los capítulos **2 ¿Qué es IAM?**, **3 Conceptos básicos** y **4 Funciones**. |
| 2019-03-05 | Esta edición es el quinto lanzamiento oficial.<br>Agregado capítulo **8 Notas y restricciones**. |
| 2019-02-20 | Esta edición es el cuarto lanzamiento oficial.<br>Agregado capítulo **3 Conceptos básicos**. |
| 2019-01-15 | Esta edición es el tercer lanzamiento oficial.<br>Agregado capítulo **5 Servicios en la nube compatibles**. |
| 2018-08-10 | Esta versión es el segundo lanzamiento oficial, que incorpora el siguiente cambio:<br>Agregado "Protección de Datos Personales". |
| 2018-03-30 | Esta edición es el primer lanzamiento oficial. |