Descripción general del servicio

Descripción general del servicio

Edición 01

Fecha 2022-11-08

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 Infografías

2 ¿Qué es IAM?

Identity and Access Management (IAM) es un servicio básico de Huawei Cloud que 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.

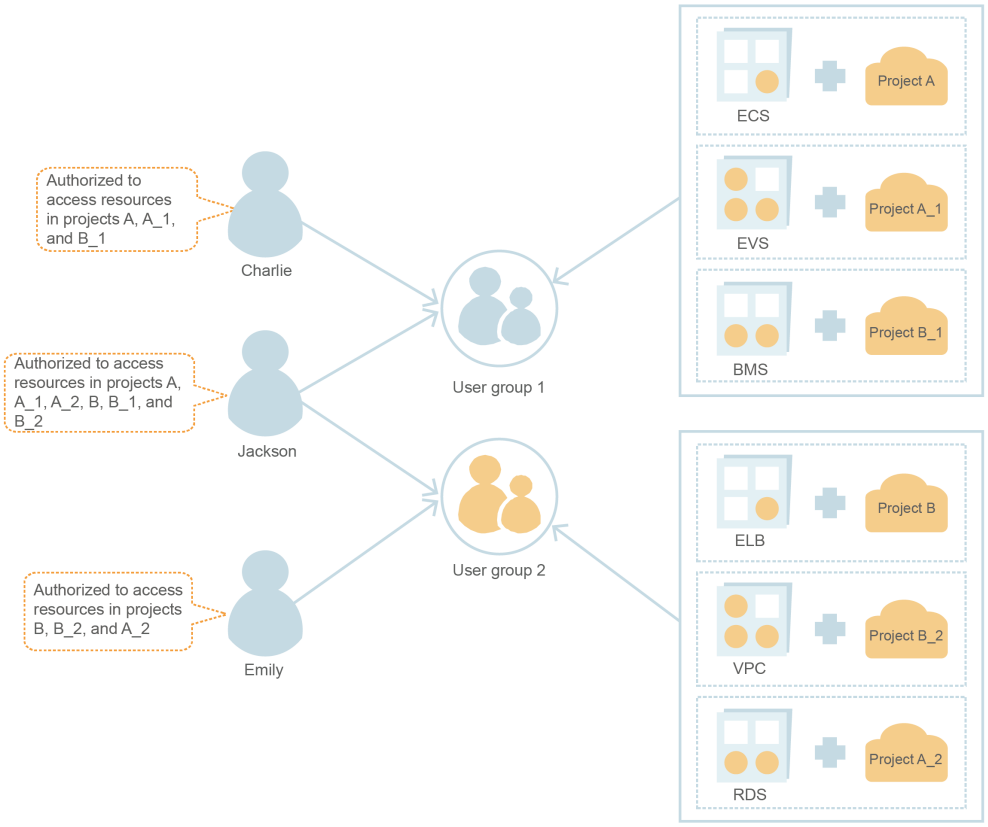
Ventajas

Control de acceso detallado para los recursos de Huawei Cloud

Se crea una cuenta después de registrarse con éxito en Huawei Cloud. 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 en Huawei Cloud,, como Elastic Cloud Servers (ECSs), Elastic Volume Services (EVSs), y Bare Metal Servers (BMSs), para diferentes equipos o aplicaciones en su empresa, puede crear usuarios de IAM para los miembros del equipo o las aplicaciones y concederles los permisos necesarios para completar las tareas. Los usuarios de IAM utilizan sus propios nombres de usuario y contraseñas para iniciar sesión en la Huawei Cloud y acceder a los recursos de su cuenta.

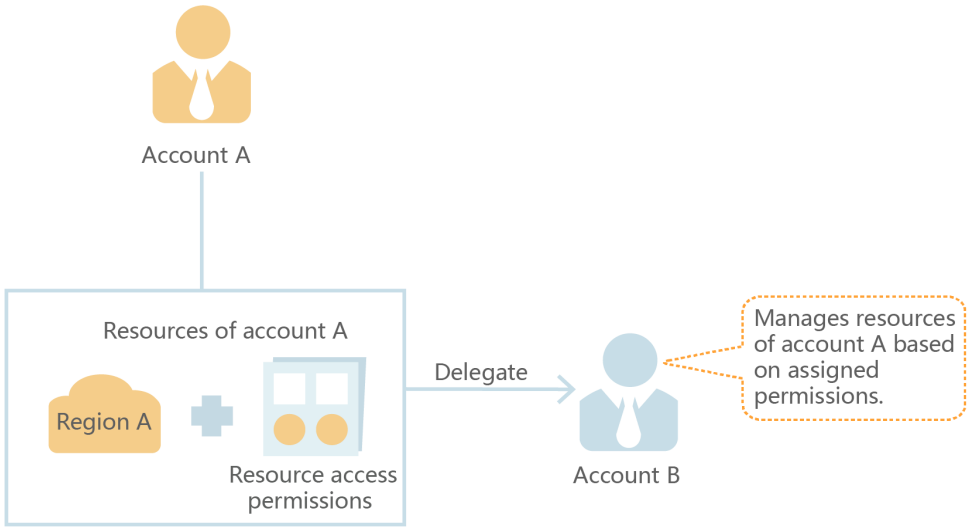
Además de IAM, puede usar Enterprise Management para controlar el acceso a los recursos de la nube. Enterprise Management admite una gestión de permisos más detallada y una gestión de proyectos empresariales. Puede elegir entre IAM o Enterprise Management para satisfacer sus necesidades. Para obtener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



Delegación de acceso a recursos entre cuentas

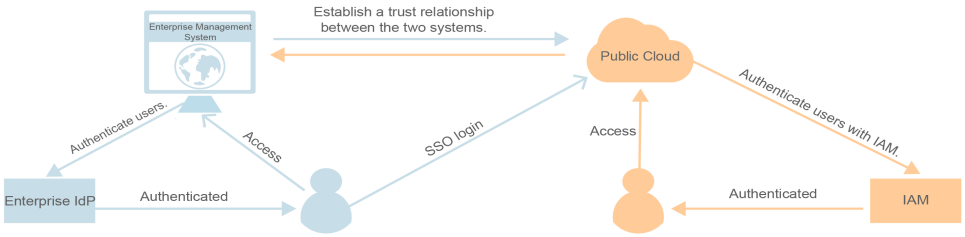
Si compra varios recursos en Huawei Cloud, puede delegar otra cuenta para gestionar recursos específicos para una operación eficiente.

Por ejemplo, crea una agencia para una empresa profesional de O&M para gestionar recursos específicos con la propia cuenta de la empresa. Puede cancelar o modificar los permisos delegados en cualquier momento si la delegación cambia. En la siguiente figura, la cuenta A es la parte delegada, y la cuenta B es la parte delegada.



Acceso federado a Huawei Cloud con cuentas empresariales existentes

Si su empresa tiene un sistema de identidad, puede crear un proveedor de identidad en IAM para proporcionar acceso de single sign-on (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**.

- **REST APIs**

  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.

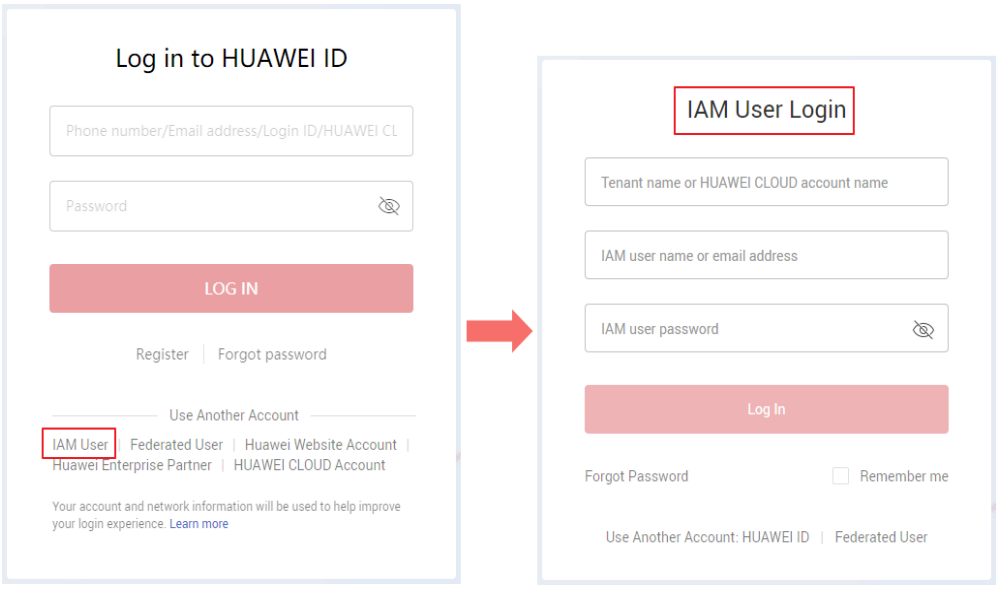
No puede modificar o eliminar su cuenta en IAM, pero puede hacerlo en My Account.

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 (contraseña y 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, el usuario puede restablecer la contraseña consultando **¿Qué puedo hacer si se olvida mi contraseña?**

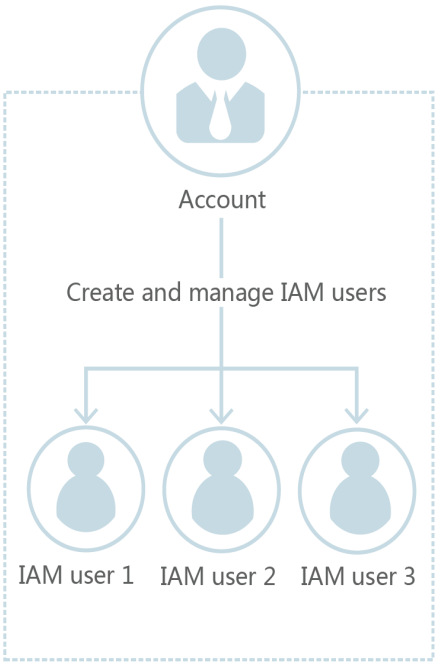
Figura 3-1 Inicio de sesión de usuario de IAM



Relación entre una cuenta y sus usuarios de IAM

Una cuenta y sus usuarios de IAM comparten una relación padre-hijo. La cuenta es propietaria de los recursos y realiza pagos por los recursos utilizados por los usuarios de IAM. Tiene permisos completos para estos recursos. Los usuarios de IAM se crean mediante una cuenta y solo tienen los permisos otorgados por la cuenta. El administrador de la cuenta puede modificar o cancelar los permisos de los usuarios de IAM en cualquier momento.

Figura 3-2 Usuarios de cuenta e IAM



Autorización

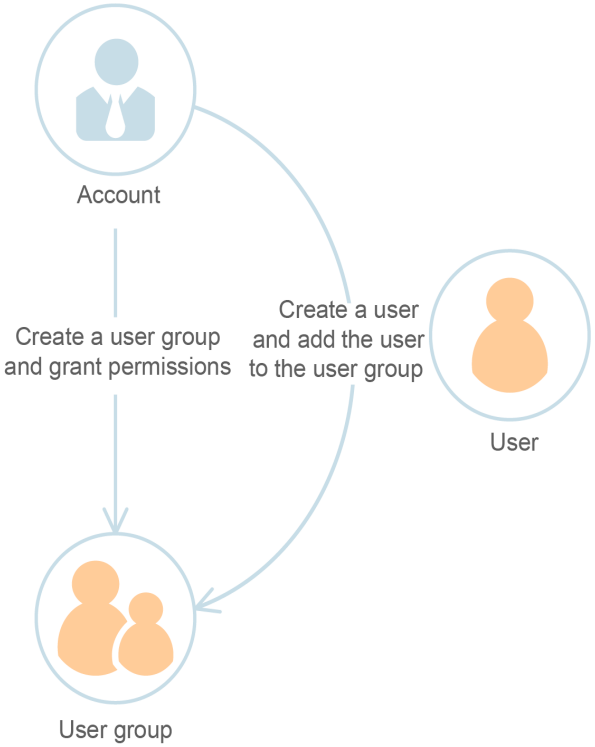
La autorización es el proceso de concesión de permisos necesarios para que un usuario realice una tarea.

Grupo de usuarios

Puede utilizar grupos de usuarios para asignar permisos a los usuarios de IAM. 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 asignados a todos estos grupos.

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

Figura 3-3 Grupo de usuarios y usuarios



Permiso

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define permisos de nivel de servicio en función de las responsabilidades del usuario. Solo hay un número limitado de roles para conceder permisos a los usuarios.
- Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas condiciones. Este mecanismo permite una autorización basada en políticas más flexible y un control de acceso seguro. Por ejemplo, puede conceder a los usuarios de ECS solo los

permisos necesarios para gestionar un determinado tipo de recursos de ECS. IAM admite políticas personalizadas y definidas por el sistema.

- A **system-defined policy** defines the common actions of a cloud service. 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 agencia 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. **Envíe un ticket de servicio** y solicite que los permisos para el servicio estén disponibles en IAM.
- Puede crear **custom policies** mediante las acciones admitidas por los servicios en la nube y utilizar políticas personalizadas para complementar las políticas definidas por el sistema para un control de acceso más refinado. Puede crear políticas personalizadas en el editor visual o en la vista JSON.

Figura 3-4 Ejemplo de permisos

```
{
    "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 incluyen una contraseña y claves de acceso. Puede gestionar sus credenciales y las credenciales de los usuarios de IAM que haya creado.

- Contraseña: Una credencial común para iniciar sesión en la consola de gestión o llamar 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 llamar 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.

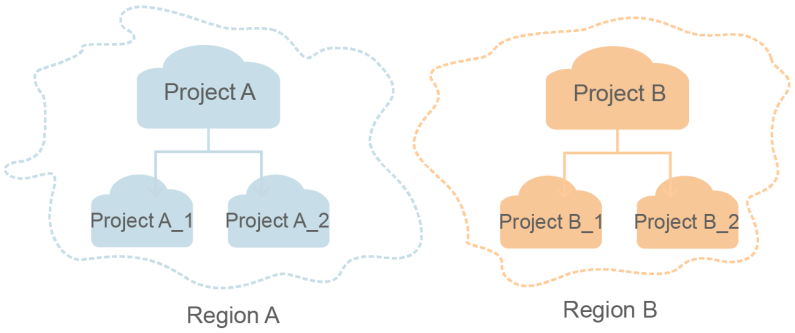
Dispositivo MFA virtual

Un dispositivo MFA virtual es una aplicación que genera códigos de verificación de 6 dígitos de acuerdo con el estándar de Time-based One-time Password Algorithm. Los dispositivos MFA pueden estar basados en hardware o software. Actualmente, Huawei Cloud admite dispositivos MFA virtuales basados en software, que son programas de aplicación que se ejecutan en dispositivos inteligentes como teléfonos móviles. Para obtener más información sobre 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 preciso, puede crear subproyectos en 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 Proyecto



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 identificadores y características de proyecto empresarial, consulte la **Guía del usuario de gestión de empresa**.

Agencia

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 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.

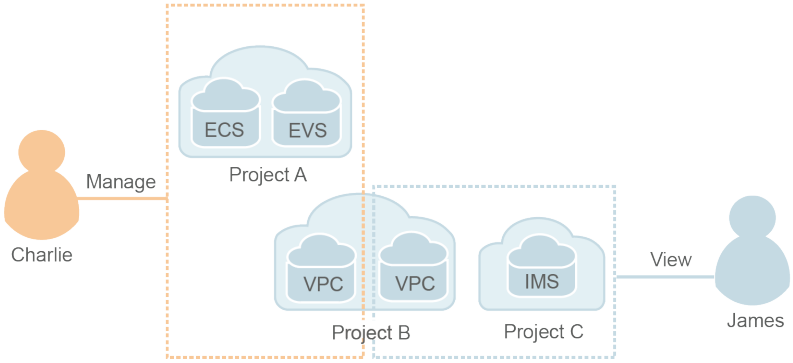
4 Funciones

IAM proporciona las siguientes funciones: gestión de permisos perfeccionada, acceso seguro, protección de operaciones críticas, asignación de permisos basados en grupos de usuarios, aislamiento de recursos basado en proyectos, autenticación de identidad federada, delegación de gestión de recursos y configuración de seguridad de cuenta.

Gestión de permisos refinados

Puede conceder a los usuarios de IAM permisos para gestionar diferentes recursos en su cuenta. Por ejemplo, a Charlie solo se le conceden los permisos necesarios para gestionar los recursos de Virtual Private Cloud (VPC) en el proyecto B.

Figura 4-1 Modelo de gestión de permisos



Acceso seguro

En lugar de compartir la contraseña de su cuenta 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. A continuación, cada usuario hereda los permisos de los grupos de los que es miembro. 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 aislar recursos.

Autenticación de identidad federada

La función de autenticación de identidad federada permite a las empresas con sistemas de autenticación de identidad acceder a Huawei Cloud a través del single sign-on (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.

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 Huawei Cloud's centros de datos 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 de sistema**. **Para los servicios que no son compatibles con IAM, solo puede usar su cuenta para acceder a estos servicios.**

- Servicio: Nombre de un servicio en la nube que admite la gestión de permisos mediante IAM. **Haga clic en el enlace del nombre del servicio para ver los permisos admitidos por el servicio.**
- Ámbito: la región donde se pueden asignar permisos de acceso para un servicio mediante IAM.
  - Región global: Los servicios desplegados sin especificar regiones físicas se denominan servicios globales. Los permisos para estos servicios deben asignarse en la región Global. Los usuarios no necesitan cambiar de región cuando acceden a estos servicios.
  - Regiones específicas: Los servicios desplegados en 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: Indica si un servicio admite la gestión de permisos mediante la consola de IAM.
- API: Indica si un servicio admite la gestión de permisos mediante API.
- Agencia: Indica si se puede delegar un servicio para acceder y gestionar otros servicios en la nube en su nombre.
- Directiva: Indica 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: Indica si un servicio soporta autorización por proyecto empresarial. Para obtener más información acerca de los proyectos de empresa, consulte **Guía de usuario de Enterprise Management**.

NOTA

√: supported; x: not supported

Cómputo

Servicio	Alcance	Consola	API	Agencia	Política	Proyecto empresarial
Elastic Cloud Server (ECS)	Regiones específicas	√	√	√	√	√
Bare Metal Server (BMS)	Regiones específicas	√	√	√	√	√
Auto Scaling (AS)	Regiones específicas	√	√	x	√	√
Cloud Phone (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	Agencia	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)	Global	√	√	√	√	√
Scalable File Service (SFS)	Regiones específicas	√	√	x	√	√

Servicio	Alcance	Consola	API	Agencia	Política	Proyecto empresarial
Content Delivery Network (CDN)	Global	√	√	x	√	√
Cloud Backup and Recovery (CBR)	Regiones específicas	√	√	x	√	√

Red

Servicio	Alcance	Consola	API	Agencia	Política	Proyecto empresarial
Virtual Private Cloud (VPC)	Regiones específicas	√	√	x	√	√
Elastic Load Balance (ELB)	Regiones específicas	√	√	x	√	√
Domain Name Service (DNS)	Global	√	√	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	Agencia	Política	Proyecto empresarial
Cloud Container Engine (CCE)	Regiones específicas	√	√	x	√	√

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

Servicio	Alcance	Consola	API	Agencia	Política	Proyecto empresarial
Advanced Anti-DDoS (AAD)	Regiones específicas	√	√	√	x	√
Cloud Native Anti-DDoS (CNAD)	Global	√	√	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)	Global	√	√	x	√	x
Container Guard Service (CGS)	Regiones específicas	√	x	x	√	x
Situation Awareness (SA)	Global	√	√	√	√	x
Cloud Bastion Host (CBH)	Regiones específicas	√	√	x	√	x
Data Security Center (DSC)	Regiones específicas	√	√	x	√	x

Gestión & Gobernanza

Servicio	Alcance	Consola	API	Agencia	Política de grano fino	Proyecto empresarial
Identity and Access Management (IAM)	Global	√	√	x	√	x
Cloud Eye	Regiones específicas	√	√	x	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)	Global	√	√	x	x	x

Aplicación

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

Servicio	Alcance	Consola	API	Agencia	Política	Proyecto empresarial
Distributed Message Service for RabbitMQ (DMS for RabbitMQ)	Regiones específicas	√	√	x	√	√
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	Agencia	Política	Proyecto empresarial
Dedicated Distributed Storage Service (DSS)	Regiones específicas	√	√	x	√	x

Migración

Servicio	Alcance	Consola	API	Agencia	Política	Proyecto empresarial
Server Migration Service (SMS)	Global	√	x	x	√	x

Servicio	Alcance	Consola	API	Agencia	Política	Proyecto empresarial
Object Storage Migration Service (OMS)	Regiones específicas	√	x	x	x	x
Cloud Data Migration (CDM)	Regiones específicas	√	√	√	√	√

Borde Inteligente

Servicio	Alcance	Consola	API	Agencia	Política	Proyecto empresarial
Intelligent EdgeCloud (IEC)	Global	√	x	x	√	x

EI

Servicio	Alcance	Consola	API	Agencia	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	√

Servicio	Alcance	Consola	API	Agencia	Política de grano fino	Proyecto empresarial
Cloud Search Service (CSS)	Regiones específicas	√	√	√	x	√
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	Agencia	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	Agencia	Política	Proyecto empresarial
Voice Call	Regiones específicas	√	√	√	x	x
Message & SMS	Regiones específicas	√	√	√	x	x
Private Number	Regiones específicas	√	√	√	√	x

Video

Servicio	Alcance	Consola	API	Agencia	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	Agencia	Política	Proyecto empresarial
DevCloud	Regiones específicas	√	x	x	√	√
ProjectMan	Regiones específicas	√	√	x	√	x
CloudIDE	Regiones específicas	√	√	x	√	x

Soporte para el usuario

Servicio	Alcance	Consola	API	Agencia	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 Management	Global	√	√	x	√	x
Service Tickets	Global	√	√	x	x	x
ICP License Service	Global	√	x	x	x	x
Professional Services	Global	√	x	x	√	x

Otros

Servicio	Alcance	Consola	API	Agencia	Política	Proyecto empresarial
Message Center	Regiones específicas	√	x	x	√	x

6 Mecanismo de protección de datos personales

Para evitar que entidades o personas no autorizadas accedan a datos personales, como el nombre de usuario, la contraseña y el número de teléfono móvil, IAM cifra los datos antes de almacenarlos. IAM también controla el acceso a los datos y registra todas las operaciones realizadas en los datos.

Datos personales

Tabla 6-1 enumera los datos personales generados o recopilados por IAM.

Tabla 6-1 Datos personales

Tipo	Origen	Modificable	Obligatorio
Nombre de usuario.	● Se introduce cuando se crea un usuario en la consola de gestión. ● Se introduce cuando se llama a una API.	No	Sí 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. ● Se introduce cuando se llama a una API.	Sí	No También puede elegir la autenticación AK/SK.
Dirección de correo	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.	Sí	No

Tipo	Origen	Modificable	Obligatorio
Número de móvil	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.	Sí	No
AK/SK	Creado en la página **My Credentials** o en la consola de IAM.	No AK/SK no se puede modificar, pero se pueden eliminar y crear de nuevo.	No AK/SK se utilizan para firmar las solicitudes enviadas a las API de llamada.

Almacenamiento de datos personales

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.
- Contraseñas, direcciones de correo electrónico, números de móvil y SK: datos confidenciales, que se cifran antes del almacenamiento.

Control de acceso

Los datos personales se almacenan en la base de datos de IAM después de ser cifrados. El acceso a la base de datos se controla a través del mecanismo de lista blanca.

Autenticación MFA

Puede habilitar la protección de inicio de sesión y la protección de operaciones críticas seleccionando **Security Settings** > **Critical Operations**. Si habilita estas funciones, los usuarios de su cuenta deben verificar su identidad por SMS, correo electrónico o dispositivo MFA virtual antes de iniciar sesión o realizar una operación crítica.

Restricciones de API

- Se requiere autenticación AK/SK para llamar a las API. Puede crear una clave de acceso (AK/SK) y descargar el archivo que contiene la clave de acceso. Si no puede localizar el archivo, puede crear una clave de acceso de nuevo y descargar el archivo. No comparta su clave de acceso con nadie más.
- IAM no proporciona API para realizar consultas por lotes y modificar datos personales.

Registros de operaciones

IAM registra todas las operaciones de datos personales, incluyendo la adición, modificación, consulta y eliminación de datos personales. Sube los registros de operaciones a CTS, y permite a los usuarios consultar solo sus propios registros de operaciones.

7 Gestión de 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 soportados por IAM, consulte **Permisos de sistema**.

Permisos de IAM

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

IAM es un servicio global al que puede acceder desde todas las regiones. Puede asignar permisos de IAM a los usuarios del proyecto de servicio global. De esta manera, los usuarios no necesitan cambiar regiones cuando acceden a IAM.

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define permisos de nivel de servicio en función de las responsabilidades del usuario. Solo hay un número limitado de roles para conceder permisos a los usuarios. Cuando concede permisos mediante roles, también debe asignar roles de dependencia.
- Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas condiciones. Este mecanismo permite una autorización basada en políticas más flexible y un control de acceso seguro. Por ejemplo, puede conceder a los usuarios de ECS solo los permisos necesarios para gestionar un determinado tipo de recursos de ECS. La mayoría de las políticas 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 7-1 enumera todas las funciones y políticas definidas por el sistema admitidas por IAM.

Tabla 7-1 Funciones y políticas definidas por el sistema compatibles con 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.	System-defined policy	**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.	System-defined policy	**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.	System-defined role	**Contenido del rol de administrador de seguridad**
Agent Operator	Operador IAM (parte delegada) con permisos para cambiar roles y recursos de acceso de una parte delegada.	System-defined role	**Contenido del rol de operador de agente**
Tenant Guest	Permisos de sólo lectura para todos los servicios excepto IAM.	System-defined policy	**Contenido del rol de invitado del inquilino**
Tenant Administrator	Permisos de administrador para todos los servicios excepto IAM.	System-defined policy	**Contenido del rol de Administrador del inquilino**

Tabla 7-2 enumera las operaciones comunes admitidas por cada política o rol definido por el sistema de IAM. Elija las políticas o roles adecuados según sea necesario.

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 7-2 Operaciones comunes admitidas por políticas o roles definidos por el sistema

Operación	Administrador de seguridad	Agente Operador	FullAccess	IAM ReadOnlyAccess
Creación de usuarios de IAM	Sí	No	Sí	No

Operación	Administrador de seguridad	Agente Operador	FullAccess	IAM ReadOnlyAccess
Consultar los detalles del usuario de IAM	Sí	No	Sí	Sí
Modificación de la información de usuario de IAM	Sí	No	Sí	No
Consultar la configuración de seguridad de los usuarios de IAM	Sí	No	Sí	Sí
Modificación de la configuración de seguridad de los usuarios de IAM	Sí	No	Sí	No
Eliminación de usuarios de IAM	Sí	No	Sí	No
Creación de grupos de usuarios	Sí	No	Sí	No
Consultar los detalles del grupo de usuarios	Sí	No	Sí	Sí
Modificación de la información del grupo de usuarios	Sí	No	Sí	No
Adición de usuarios a grupos de usuarios.	Sí	No	Sí	No

Operación	Administrador de seguridad	Agente Operador	FullAccess	IAM ReadOnlyAccess
Eliminar usuarios de grupos de usuarios	Sí	No	Sí	No
Eliminar grupos de usuarios	Sí	No	Sí	No
Asignar permisos a grupos de usuarios	Sí	No	Sí	No
Eliminación de permisos de grupos de usuarios	Sí	No	Sí	No
Creación de políticas personalizadas	Sí	No	Sí	No
Modificación de políticas personalizadas	Sí	No	Sí	No
Eliminación de políticas personalizadas	Sí	No	Sí	No
Consultar detalles de permisos	Sí	No	Sí	Sí
Creación de agencias	Sí	No	Sí	No
Consulta de agencias	Sí	No	Sí	Sí
Modificación de agencias	Sí	No	Sí	No
Cambio de roles	No	Sí	Sí	No
Elimianción de agencias	Sí	No	Sí	No

Operación	Administrador de seguridad	Agente Operador	FullAccess	IAM ReadOnlyAccess
Concesión de permisos a agencias	Sí	No	Sí	No
Eliminación de los permisos de las agencias	Sí	No	Sí	No
Creación de proyectos	Sí	No	Sí	No
Consulta de proyectos	Sí	No	Sí	Sí
Modificación de proyectos	Sí	No	Sí	No
Supresión de proyectos	Sí	No	Sí	No
Creación de proveedores de identidad	Sí	No	Sí	No
Importación de archivos de metadatos	Sí	No	Sí	No
Consultar archivos de metadatos	Sí	No	Sí	Sí
Consulta de proveedores de identidad	Sí	No	Sí	Sí
Consulta de protocolos	Sí	No	Sí	Sí
Consulta de asignaciones	Sí	No	Sí	Sí
Actualización de proveedores de identidad	Sí	No	Sí	No
Actualización de protocolos	Sí	No	Sí	No

Operación	Administrador de seguridad	Agente Operador	FullAccess	IAM ReadOnlyAccess
Actualización de asignaciones	Sí	No	Sí	No
Supresión de proveedores de identidad	Sí	No	Sí	No
Supresión de protocolos	Sí	No	Sí	No
Supresión de asignaciones	Sí	No	Sí	No
Consulta de cuotas	Sí	No	Sí	No

Solo los administradores pueden gestionar las claves de acceso cuando está habilitada **gestión de clave de acceso**. Si los usuarios de IAM necesitan crear, habilitar, deshabilitar o eliminar sus propias claves de acceso, deben pedírselo al administrador a **deshabilitar gestión de clave de acceso** La gestión de claves de acceso está deshabilitada de forma predeterminada.

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 7-3 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)	Sí	No	Sí	No
Consulta de claves de acceso (para otros usuarios de IAM)	Sí	No	Sí	Sí

Operación	Administrador de seguridad	Agente Operador	FullAccess	IAM ReadOnlyAccess
Modificación de claves de acceso (para otros usuarios de IAM)	Sí	No	Sí	No
Eliminación de claves de acceso (para otros usuarios de IAM)	Sí	No	Sí	No

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 inquilino

```
{
    "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 inquilino

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



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

8 Notas y restricciones

En la siguiente tabla se enumeran las cuotas de varios recursos en IAM. La marca " √ " indica que puede aumentar la cuota para cumplir con los requisitos de servicio. Para obtener más información, consulte **¿Cómo Aumento Mi Cuota?**

Artículo	Límite	Cambiable
usuarios de IAM	50	√
Grupos de usuarios	20	√
Número máximo de usuarios que se pueden agregar a un grupo de usuarios	Número de usuarios de IAM que se han creado con su cuenta	x
Delegaciones	50	√
Número de grupos a los que se puede agregar un usuario	10	x
Número de pares AK/SK que un usuario puede crear	2	x
Número de dispositivos MFA virtuales que pueden enlazarse a un usuario	1	x
Políticas personalizadas	200	√
Número de permisos (incluidas las políticas y roles definidos por el sistema y las políticas personalizadas) que se pueden enlazar a un grupo de usuarios basado en proyectos de IAM	200	√
Número de permisos (incluidas las políticas y roles definidos por el sistema y las políticas personalizadas) que se pueden vincular a una agencia	200	√

Artículo		Límite	Cambiable
Número de permisos (incluidas las directivas y roles definidos por el sistema y las directivas personalizadas) que se pueden enlazar a un grupo de usuarios basado en proyectos de empresa		500	√
Número de permisos (incluidas las políticas y roles definidos por el sistema y las políticas personalizadas) que se pueden enlazar a un usuario en función de proyectos de empresa		500	√
Número de subproyectos en cada región		10	√
Número de caracteres permitidos en un nombre de usuario		32	x
Número de caracteres permitidos en un nombre de grupo de usuarios		64	x
Número de caracteres permitidos en un nombre de política		64	x
Política personalizada	Número máximo de caracteres	6144	x
	Número máximo de declaraciones	Hasta 8 estados de cuenta por política	x
	Acciones	Hasta 100 acciones por sentencia	x
	Recursos	Hasta 10 recursos por estado de cuenta	x
	Condiciones	Hasta 10 condiciones por sentencia	x
Número de caracteres permitidos en el nombre de una agencia		64	x
Proveedores de identidades	Cantidad	10	√
	Número máximo de caracteres que se pueden contener en el nombre de un proveedor de identidad	64	x

Artículo		Límite	Cambiable
	Número total de reglas de asignación de todos los proveedores de identidad de una cuenta	10	√

9 Historial de cambios

Tabla 9-1 Historial de cambios

Fecha	Descripción
2021-12-01	Esta versión es el decimoséptimo lanzamiento oficial, que incorpora el siguiente cambio: Agregó la cuota de regla de conversión de identidad en **Notas y restricciones**.
2021-11-23	Esta edición es la decimosexta versión oficial, que incorpora el siguiente cambio: Agregó la descripción de los proyectos de empresa en **Servicios en la nube compatibles**.
2021-04-25	Esta versión es el decimoquinto lanzamiento oficial, que incorpora el siguiente cambio: Agregó cuotas de permisos en **Notas y restricciones**.
2020-12-30	Esta edición es la decimocuarta versión oficial, que incorpora el siguiente cambio: Se han actualizado las capturas de pantalla en **Conceptos Básicos** en función del cambio en el método de inicio de sesión.
2020-11-30	Esta edición es la decimotercera versión oficial, que incorpora el siguiente cambio: Se actualizó 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: Se han actualizado las capturas de pantalla en **Conceptos Básicos** en función del 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: Agregó una sección **Gestión de permisos**.
2020-06-11	Esta versión es el décimo lanzamiento oficial, que incorpora el siguiente cambio: Se ha cambiado el número máximo de grupos de usuarios a los que se puede agregar un usuario a **10** en **Notas y restricciones**.
2020-06-08	Este versión es el noveno lanzamiento oficial, que incorpora el siguiente cambio: Se agregaron descripciones sobre HUAWEI ID en **Conceptos Básicos** y se actualizaron 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: ● Optimizó la descripción de los permisos en **Conceptos Básicos**. ● Agregó el límite de subproyectos en una región en **Notas y restricciones**.
2019-11-20	Esta versión es el séptimo lanzamiento oficial, que incorpora el siguiente cambio: Aumento de la cuota de política personalizada a 200 en **Notas y restricciones**.
2019-06-05	Esta edición es el sexto lanzamiento oficial. Descripciones modificadas en capítulo **¿Qué es IAM?**, **Conceptos Básicos**, y **Funciones**.
2019-03-05	Esta edición es el quinto lanzamiento oficial. Agregó capítulo **Notas y restricciones**.
2019-02-20	Esta edición es el cuarto lanzamiento oficial. Agregó capítulo **Conceptos Básicos**.
2019-01-15	Esta edición es el tercer lanzamiento oficial. Agregó capítulo **Servicios en la nube compatibles**.
2018-08-10	Esta versión es el segundo lanzamiento oficial. Agregó capítulo **Mecanismo de protección de datos personales**.
2018-03-30	Esta versión es el primer lanzamiento oficial.

