IAM

Service Overview

Edição 01

Data 03-04-2023

HUAWEI TECHNOLOGIES CO., LTD.

Marcas registadas e permissões


e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

Huawei Technologies Co., Ltd.

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

Site: https://www.huawei.com

Email: support@huawei.com

Índice

1 Infográficos

2 O que é o IAM?

O Identity and Access Management (IAM) da Huawei Cloud fornece gerenciamento de permissões para ajudá-lo a controlar com segurança o acesso aos seus serviços e recursos de nuvem.

O IAM é gratuito. Você paga apenas pelos recursos da nuvem em sua conta.

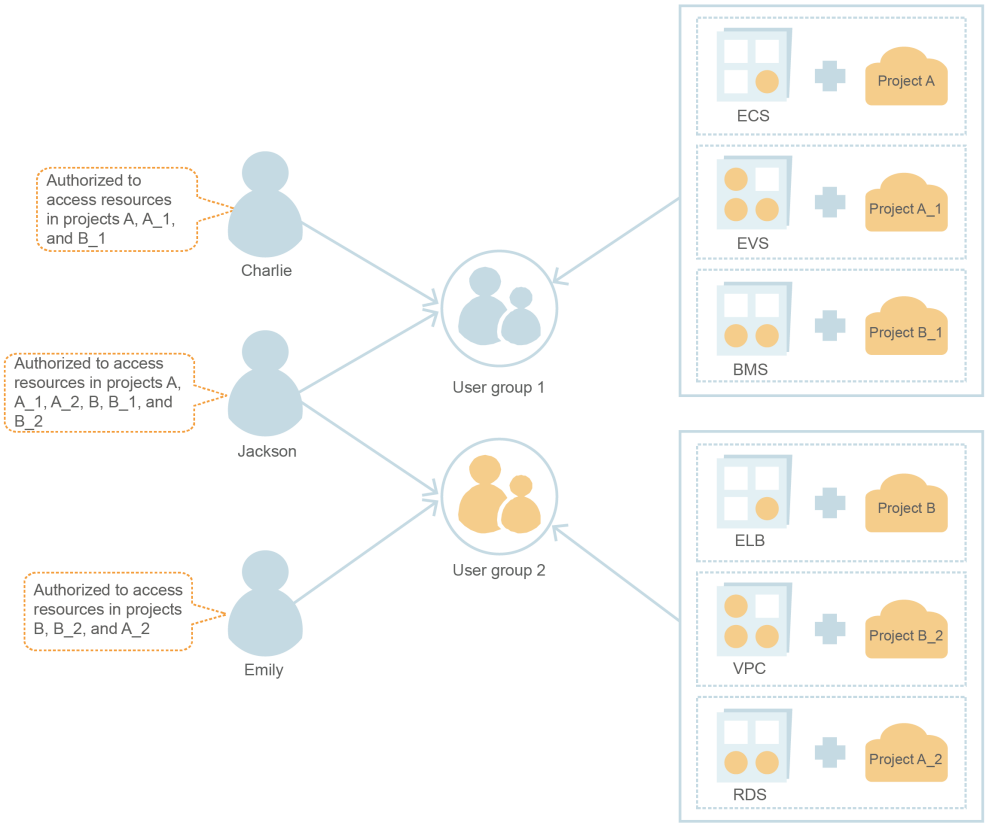
Vantagens

Controle de acesso refinado para recursos da Huawei Cloud

Quando você se registra com sucesso na Huawei Cloud, sua conta é criada automaticamente. Sua conta possui recursos e paga pelo uso desses recursos. Sua conta tem permissões de acesso total aos seus serviços e recursos de nuvem.

Se você comprar vários recursos da Huawei Cloud, como Elastic Cloud Servers (ECSs), Elastic Volume Services (EVSs) e Bare Metal Servers (BMSs), para diferentes equipes ou aplicações em sua empresa, poderá usar sua conta para criar usuários do IAM para os membros da equipe ou aplicações e conceder a eles as permissões necessárias para concluir tarefas específicas. Os usuários do IAM usam seus próprios nomes de usuário e senhas para fazer logon na Huawei Cloud e acessar os recursos em sua conta.

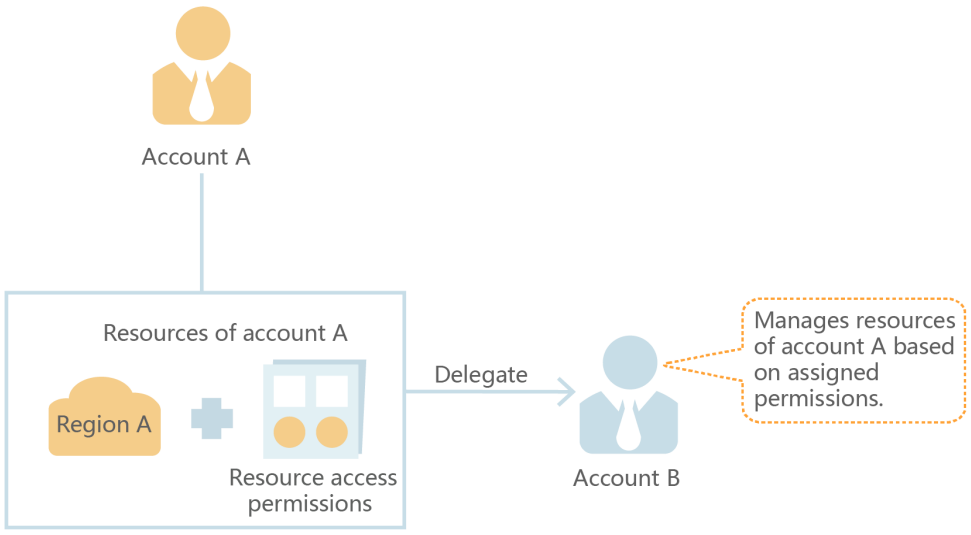
Além do IAM, você pode usar o Enterprise Management para controlar o acesso aos recursos da nuvem. O Enterprise Management oferece suporte ao gerenciamento de permissões mais refinado e ao gerenciamento de projetos empresariais. Você pode escolher o IAM ou o Enterprise Management para atender às suas necessidades. Para obter detalhes, consulte **Quais são as diferenças entre o IAM e o Enterprise Management?**



Delegação de acesso a recursos entre contas

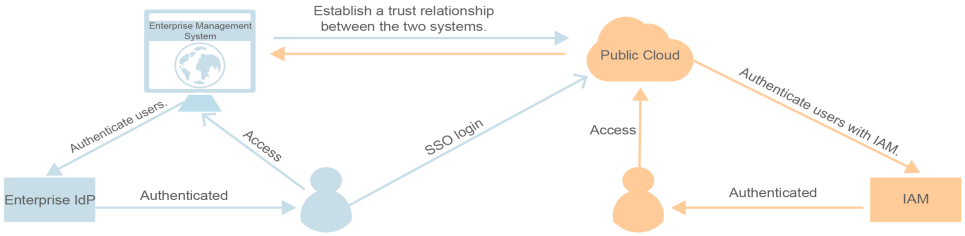
Se você comprar vários recursos da Huawei Cloud, poderá delegar outra conta para gerenciar alguns de seus recursos para uma O&M eficiente.

Por exemplo, você pode criar uma agência para uma empresa profissional de O&M para permitir que a empresa gerencie recursos específicos com a própria conta da empresa. Se a delegação for alterada, você poderá modificar ou revogar as permissões delegadas a qualquer momento. Na figura a seguir, a conta A é a parte delegante e a conta B é a parte delegada.



Acesso federado à Huawei Cloud com contas empresariais existentes (federação de identidade)

Se a sua empresa tiver um sistema de identidade, você poderá criar um provedor de identidade (IdP) no IAM para fornecer acesso de logon único (SSO) à Huawei Cloud para os funcionários em sua empresa. O provedor de identidade estabelece uma relação de confiança entre a sua empresa e a Huawei Cloud, permitindo que funcionários acessem a Huawei Cloud usando as suas contas existentes.



Métodos de acesso

Você pode acessar o IAM usando um dos seguintes métodos:

- **Console de gerenciamento**

  Acesse o IAM por meio do console de gerenciamento – uma interface visual baseada em navegador. Para obter detalhes, consulte **Acesso ao console do IAM**.

- **APIs REST**

  Acesse o IAM usando APIs REST de forma programável. Para obter detalhes, consulte **Referência de API**.

3 Conceitos básicos

A seguir estão os conceitos básicos que você precisa entender antes de começar a usar o serviço IAM.

Conta

Uma conta é criada depois que você se registra com sucesso na Huawei Cloud. Sua conta é proprietária dos recursos da Huawei Cloud e paga pelo uso desses recursos. Ela tem permissões de acesso total para seus serviços e recursos de nuvem e você pode usar sua conta para executar operações como redefinir a senha de logon e atribuir permissões a usuários do IAM. Os recursos usados pelos usuários do IAM na sua conta são cobrados na sua conta.

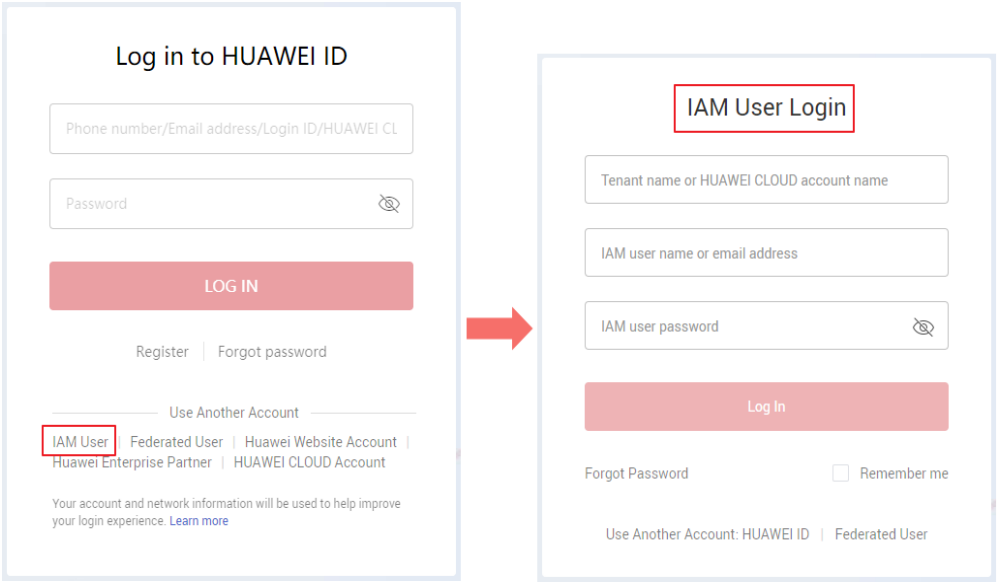
Você não pode modificar ou excluir sua conta no IAM, mas você pode fazer isso em Minha conta.

Usuário do IAM

Você pode usar sua conta para criar usuários do IAM e atribuir permissões para recursos específicos. Cada usuário do IAM tem suas próprias credenciais de identidade (senha ou chaves de acesso) e usa recursos de nuvem com base nas permissões atribuídas. Os usuários do IAM não podem fazer pagamentos por conta própria. Você pode usar sua conta para pagar suas contas.

Se um usuário do IAM esquecer sua senha, ele poderá redefini-la consultando **Como redefinir minha senha?**

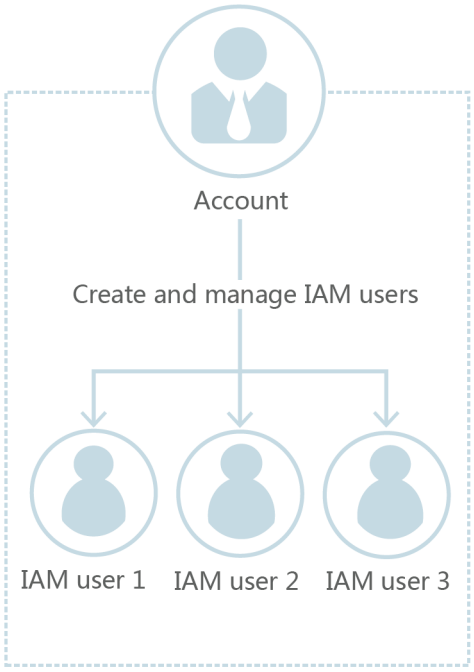
Figura 3-1 Logon de usuário do IAM



Relação entre uma conta e seus usuários do IAM

Uma conta e seus usuários do IAM têm um relacionamento pai-filho. A conta é proprietária dos recursos e faz pagamentos pelos recursos usados pelos usuários do IAM. Ela tem permissões completas para esses recursos. Os usuários do IAM são criados por uma conta e só têm as permissões concedidas pela conta. A conta pode modificar ou revogar as permissões dos usuários do IAM a qualquer momento. Os usuários do IAM não podem fazer pagamentos por conta própria. A conta paga pelos recursos que eles usam.

Figura 3-2 Conta e usuários do IAM



Autorização

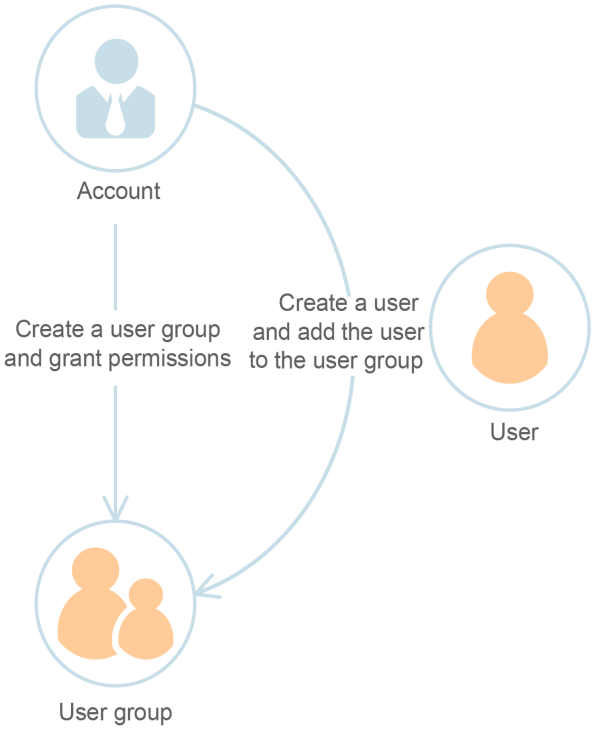
Autorização é o processo de concessão de permissões necessárias para um usuário executar tarefas específicas.

Grupo de usuários

Um grupo de usuários do IAM é uma coleção de usuários do IAM. Os grupos de usuários permitem que você especifique permissões para vários usuários, o que pode facilitar o gerenciamento das permissões para esses usuários. Os usuários do IAM adicionados a um grupo de usuários obtêm automaticamente as permissões atribuídas ao grupo. Se um usuário for adicionado a vários grupos de usuários, o usuário herdará as permissões de todos esses grupos.

Há um grupo de usuários padrão **admin**. Ele tem todas as permissões necessárias para usar todos os recursos de nuvem. Os usuários do IAM nesse grupo podem executar operações em todos os recursos, incluindo, entre outros, a criação de grupos de usuários e usuários, a atribuição de permissões e o gerenciamento de recursos.

Figura 3-3 Grupo de usuários e usuários



Permissões

Você pode conceder permissões usando funções e políticas.

- Funções: uma estratégia de autorização de alta granularidade fornecida pelo IAM para atribuir permissões com base nas responsabilidades de trabalho dos usuários. Apenas um número limitado de funções em nível de serviço está disponível para autorização.
- Políticas: uma estratégia de autorização refinada que define as permissões necessárias para realizar operações em recursos específicos de nuvem sob determinadas condições. Esse tipo de autorização é mais flexível e é ideal para acesso de privilégio mínimo. Por

exemplo, você pode conceder permissão somente aos usuários para gerenciar ECSs de um determinado tipo. O IAM oferece suporte a ambas políticas definidas pelo sistema e políticas personalizadas.

– Uma **política definida pelo sistema** define as ações comuns de um serviço de nuvem. Políticas definidas pelo sistema podem ser usadas para atribuir permissões a grupos de usuários e não podem ser modificadas. Se você precisar atribuir permissões para um serviço específico a um grupo de usuários ou agência no console do IAM, mas não conseguir encontrar políticas correspondentes, isso indicará que o serviço não oferece suporte ao gerenciamento de permissões por meio do IAM. Você pode **enviar um tíquete de serviço** para solicitar que as permissões para o serviço sejam disponibilizadas no IAM.
– As políticas personalizadas funcionam como um complemento às políticas definidas pelo sistema. Você pode criar políticas personalizadas usando as ações suportadas pelos serviços de nuvem para um controle de acesso mais refinado. Você pode criar políticas personalizadas no editor visual ou na visualização JSON.

Figura 3-4 Exemplo de permissões

Credenciais

As credenciais confirmam a identidade de um usuário quando o usuário acessa a Huawei Cloud por meio de console ou APIs. As credenciais podem ser uma senha ou chaves de acesso. Você pode gerenciar suas próprias credenciais e as credenciais de seus usuários do IAM.

- Senha: uma credencial comum para fazer logon no console de gerenciamento ou chamar APIs.
- Chave de acesso: um par de ID de chave de acesso/chave de acesso secreta (AK/SK), que só pode ser usado para chamar APIs. Cada chave de acesso fornece uma assinatura para autenticação criptográfica para garantir que as solicitações de acesso sejam secretas, completas e corretas.

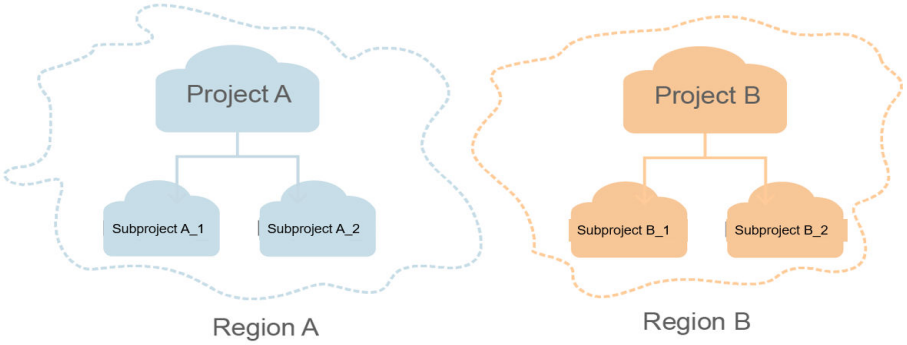
Dispositivo de MFA virtual

Um dispositivo de MFA virtual é uma aplicação que gera códigos de verificação de 6 dígitos em conformidade com o padrão TOTP (Algoritmo de senha de uso único baseado em tempo). Os dispositivos de MFA podem ser baseados em hardware ou software. A Huawei Cloud suporta apenas dispositivos de MFA virtual baseados em software, que são aplicações executadas em dispositivos inteligentes, como telefones celulares. Para obter detalhes sobre como usar dispositivos de MFA virtual, consulte **Dispositivo de MFA virtual**.

Projeto

Uma região corresponde a um projeto. Os projetos padrão são definidos para agrupar e isolar fisicamente recursos (incluindo recursos de computação, armazenamento e rede) entre regiões. Você pode conceder permissões aos usuários em um projeto padrão para acessar todos os recursos na região vinculada ao projeto. Se precisar de um controlo de acesso mais refinado, pode criar subprojetos em um projeto padrão e comprar recursos em subprojetos. Em seguida, você pode atribuir permissões necessárias para que os usuários acessem apenas recursos em subprojetos específicos.

Figura 3-5 Projetos



Projeto empresarial

Os projetos empresariais permitem que você agrupe e gerencie recursos entre regiões. Os recursos em projetos empresariais são logicamente isolados uns dos outros. Um projeto empresarial pode conter recursos de várias regiões e você pode facilmente adicionar ou remover recursos de projetos empresariais.

Para obter detalhes sobre como obter IDs e recursos de projetos empresariais, consulte o **Guia de usuário do Enterprise Management**.

Agência

Uma relação de confiança que você pode estabelecer entre sua conta e outra conta ou um serviço de nuvem para delegar acesso a recursos.

- Delegação de conta: você pode delegar outra conta para implementar O&M em seus recursos com base nas permissões atribuídas.
- Delegação de serviços em nuvem: os serviços da Huawei Cloud interagem entre si e alguns serviços de nuvem dependem de outros serviços. Você pode criar uma agência para delegar um serviço de nuvem para acessar outros serviços.

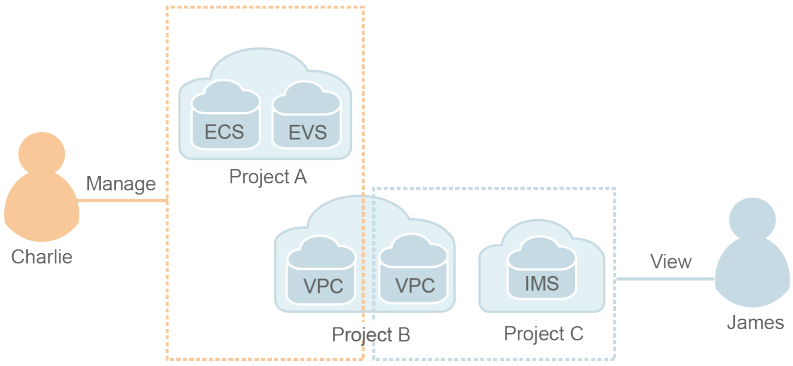
4 Funções

O IAM fornece uma variedade de funções para você proteger o acesso aos seus recursos.

Gerenciamento de permissões refinado

Você pode conceder aos usuários do IAM permissões para gerenciar diferentes recursos em sua conta. Conforme mostrado na figura a seguir, você pode conceder permissão ao Charlie para gerenciar recursos da Virtual Private Cloud (VPC) no projeto B e conceder permissão ao James apenas para visualizar recursos de VPC no projeto B.

Figura 4-1 Modelo de gerenciamento de permissões



Acesso seguro

Em vez de compartilhar sua senha com outras pessoas, você pode criar usuários do IAM para funcionários ou aplicações em sua organização e gerar credenciais de identidade para que eles acessem com segurança recursos específicos com base nas permissões atribuídas.

Proteção de operações críticas

O IAM fornece proteção de logon e proteção de operação crítica, tornando sua conta e seus recursos mais seguros. Quando você ou os usuários criados usando sua conta fazem logon no console ou executam uma operação crítica, você e os usuários precisam concluir a autenticação por e-mail, SMS ou dispositivo de MFA virtual.

Atribuição de permissões com base em grupo de usuários

Com o IAM, você não precisa atribuir permissões a usuários individuais. Em vez disso, você pode gerenciar usuários por grupo e atribuir permissões ao grupo especificado. Cada usuário então herda permissões de seus grupos. Para alterar as permissões de um usuário, você pode remover o usuário dos grupos originais ou adicionar o usuário a outros grupos.

Isolamento de recursos baseado em projetos

Você pode criar subprojetos em uma região para que os recursos nessa região possam ser isolados uns dos outros.

Autenticação de identidade federada

Empresas com sistemas de autenticação de identidade podem acessar a Huawei Cloud por meio de logon único (SSO), eliminando a necessidade de criar usuários na Huawei Cloud.

Delegação de gerenciamento de recursos

Você pode delegar contas mais profissionais e eficientes ou outros serviços de nuvem para gerenciar recursos específicos em sua conta.

Configurações de segurança da conta

As políticas de autenticação de logon e senha e a lista de controle de acesso (ACL) melhoram a segurança das informações do usuário e dos dados do sistema.

Consistência eventual

Os resultados de suas operações de IAM, como a criação de usuários e grupos de usuários e a atribuição de permissões, podem não entrar em vigor imediatamente porque os dados são replicados em diferentes servidores nos data centers da Huawei Cloud em todo o mundo. Certifique-se de que os resultados da operação tenham efeito antes de executar qualquer outra operação que dependa deles.

5 Serviços de nuvem com suporte

O IAM fornece autenticação de identidade e gerenciamento de permissões para outros serviços da Huawei Cloud. Os usuários criados no IAM podem acessar esses serviços com base nas permissões atribuídas. Para obter todas as permissões dos serviços suportados pelo IAM, consulte **Permissões definidas pelo sistema**. Para serviços que não são suportados pelo IAM, você só pode usar sua conta para acessar esses serviços.

A seguir estão listados os serviços suportados pelo IAM e as descrições de cabeçalho de tabela.

- Serviço: nome de um serviço de nuvem que oferece suporte ao gerenciamento de permissões usando o IAM.
- Escopo: a região onde as permissões de acesso para um serviço podem ser atribuídas usando o IAM.
  - Regiões globais: os serviços implementados sem especificar regiões físicas são chamados de serviços globais. As permissões para esses serviços devem ser atribuídas em regiões globais. Os usuários não precisam mudar de região quando acessam esses serviços.
  - Regiões específicas: os serviços implementados para regiões específicas são chamados de serviços em nível de projeto. As permissões para esses serviços precisam ser atribuídas em regiões específicas e entrarão em vigor apenas para as regiões correspondentes. Os usuários precisam mudar para uma dessas regiões quando acessam os serviços.
- Console: se um serviço suporta o gerenciamento de permissões usando o console do IAM.
- API: se um serviço suporta o gerenciamento de permissões usando APIs.
- Agência: se um serviço pode ser delegado para acessar e gerenciar outros serviços de nuvem em seu nome.
- Política: se um serviço suporta o gerenciamento de permissões baseado em políticas. Uma política é um conjunto de permissões que define as operações que podem ser executadas em recursos de nuvem específicos.
- Projeto empresarial: se um serviço suporta autorização por projeto empresarial. Para obter detalhes sobre projetos empresariais, consulte **Guia de usuário do Enterprise Management**.

NOTA

√: suportado; x: não suportado

Computação

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Elastic Cloud Server (ECS)	Regiões específicas	√	√	√	√	√
Bare Metal Server (BMS)	Regiões específicas	√	√	√	√	√
Auto Scaling (AS)	Regiões específicas	√	√	x	√	√
Cloud Phone Host (CPH)	Regiões específicas	√	√	x	x	x
Image Management Service (IMS)	Regiões específicas	√	√	√	√	√
FunctionGraph	Regiões específicas	√	√	√	x	√
Dedicated Host (DeH)	Regiões específicas	√	x	x	√	√

Armazenamento

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Elastic Volume Service (EVS)	Regiões específicas	√	√	x	√	√
Storage Disaster Recovery Service (SDRS)	Regiões específicas	√	√	x	x	x
Cloud Server Backup Service (CSBS)	Regiões específicas	√	√	x	x	x
Volume Backup Service (VBS)	Regiões específicas	√	√	x	x	x
Object Storage Service (OBS)	Regiões globais	√	√	√	√	√
Scalable File Service (SFS)	Regiões específicas	√	√	x	√	√

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Content Delivery Network (CDN)	Regiões globais	√	√	x	√	√
Cloud Backup and Recovery (CBR)	Regiões específicas	√	√	x	√	√

Rede

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Virtual Private Cloud (VPC)	Regiões específicas	√	√	x	√	√
Elastic Load Balance (ELB)	Regiões específicas	√	√	x	√	√
Domain Name Service (DNS)	Regiões globais	√	√	x	x	√
NAT Gateway	Regiões específicas	√	√	x	√	√
Direct Connect	Regiões específicas	√	x	x	x	x
Virtual Private Network (VPN)	Regiões específicas	√	x	x	√	x
Cloud Connect (CC)	Regiões específicas	√	x	x	√	√
VPC Endpoint (VPCEP)	Regiões específicas	√	√	x	x	x

Containers

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Cloud Container Engine (CCE)	Regiões específicas	√	√	x	√	√

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Cloud Container Instance (CCI)	Regiões específicas	√	√	x	√	√
Software Repository for Container (SWR)	Regiões específicas	√	√	x	√	x
Gene Container Service (GCS)	Regiões específicas	√	√	x	√	√

Banco de dados

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Relational Database Service (RDS)	Regiões específicas	√	√	x	√	√
Document Database Service (DDS)	Regiões específicas	√	x	x	√	√
Distributed Database Middleware (DDM)	Regiões específicas	√	√	x	√	√
Data Replication Service (DRS)	Regiões específicas	√	√	x	√	√
Data Admin Service (DAS)	Regiões específicas	√	x	x	x	x
GeminiDB	Regiões específicas	√	√	x	√	√

Segurança e conformidade

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Anti-DDoS	Regiões específicas	√	√	x	x	x

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Advanced Anti-DDoS (AAD)	Regiões específicas	√	√	√	x	√
Cloud Native Anti-DDoS (CNAD)	Regiões globais	√	√	x	√	x
Web Application Firewall (WAF)	Regiões específicas	√	x	x	x	√
Cloud Firewall (CFW)	Regiões específicas	√	x	x	√	x
Vulnerability Scan Service (VSS)	Regiões específicas	√	x	x	x	x
Host Security Service (HSS)	Regiões específicas	√	x	x	x	√
Database Security Service (DBSS)	Regiões específicas	√	x	x	√	x
Data Encryption Workshop (DEW)	Regiões específicas	√	√	x	x	x
Managed Detection and Response (MDR)	Regiões específicas	√	x	x	x	x
SSL Certificate Manager (SCM)	Regiões globais	√	√	x	√	x
Container Guard Service (CGS)	Regiões específicas	√	x	x	√	x
Situation Awareness (SA)	Regiões globais	√	√	√	√	x
Cloud Bastion Host (CBH)	Regiões específicas	√	√	x	√	x
Data Security Center (DSC)	Regiões específicas	√	√	x	√	x

Gerenciamento e governança

Serviço	Escopo	Console	API	Agência	Política refinada	Projeto empresarial
Identity and Access Management (IAM)	Regiões globais	√	√	x	√	x
Cloud Eye	Regiões específicas	√	√	x	√	√
Cloud Trace Service (CTS)	Regiões específicas	√	√	x	x	x
Application Performance Management (APM)	Regiões específicas	√	√	x	√	√
Application Operations Management (AOM)	Regiões específicas	√	√	x	√	√
Log Tank Service (LTS)	Regiões específicas	√	√	x	√	√
Tag Management Service (TMS)	Regiões globais	√	√	x	x	x

Aplicação

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
ServiceStage	Regiões específicas	√	√	x	x	x
Distributed Cache Service (DCS)	Regiões específicas	√	√	√	√	√
Distributed Message Service for Kafka (DMS for Kafka)	Regiões específicas	√	√	x	√	√
Distributed Message Service for RabbitMQ (DMS for RabbitMQ)	Regiões específicas	√	√	x	√	√

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Distributed Message Service for RocketMQ (DMS for RocketMQ)	Regiões específicas	√	√	x	√	√
Simple Message Notification (SMN)	Regiões específicas	√	√	x	x	√
Cloud Service Engine (CSE)	Regiões específicas	√	√	x	x	√
Cloud Performance Test Service (CPTS)	Regiões específicas	√	√	x	x	x
API Gateway	Regiões específicas	√	√	x	x	√
Blockchain Service (BCS)	Regiões específicas	√	√	x	√	√

DeC

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Dedicated Distributed Storage Service (DSS)	Regiões específicas	√	√	x	√	x

Migração

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Server Migration Service (SMS)	Regiões globais	√	x	x	√	x
Object Storage Migration Service (OMS)	Regiões específicas	√	x	x	x	x

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Cloud Data Migration (CDM)	Regiões específicas	√	√	√	√	√

Borda inteligente

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
CloudLake	Regiões globais	√	x	x	√	x

Inteligência empresarial

Serviço	Escopo	Console	API	Agência	Política refinada	Projeto empresarial
ModelArts	Regiões específicas	√	√	√	√	√
Data Lake Governance Center (DGC)	Regiões específicas	√	√	√	√	x
MapReduce Service (MRS)	Regiões específicas	√	√	x	√	√
Data Warehouse Service (DWS)	Regiões específicas	√	√	√	√	√
CloudTable	Regiões específicas	√	√	x	x	√
Data Lake Insight (DLI)	Regiões específicas	√	√	x	x	√
Data Ingestion Service (DIS)	Regiões específicas	√	√	√	x	√
Cloud Search Service (CSS)	Regiões específicas	√	√	√	x	√
Graph Engine Service (GES)	Regiões específicas	√	√	√	x	√

Serviço	Escopo	Console	API	Agência	Política refinada	Projeto empresarial
Recommender System (RES)	Regiões específicas	√	√	x	√	√
Moderação de conteúdo	Regiões específicas	√	√	x	√	x
Conversational Bot Service (CBS)	Regiões específicas	√	√	x	x	x
Huawei HiLens	Regiões específicas	√	x	x	√	x
Trusted Intelligent Computing Service (TICS)	Regiões específicas	√	x	x	√	x

Aplicações empresariais

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Workspace	Regiões específicas	√	√	x	x	x
ROMA Connect	Regiões específicas	√	√	√	√	√
CloudSite	Regiões específicas	√	x	√	√	x

Comunicações em nuvem

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Voice Call	Regiões específicas	√	√	√	x	x
Message & SMS	Regiões específicas	√	√	√	√	x

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Private Number	Regiões específicas	√	√	√	√	x

Vídeo

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Media Processing Center (MPC)	Regiões específicas	√	√	√	x	x
Video on Demand (VOD)	Regiões específicas	√	√	√	√	x

Desenvolvimento e O&M

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
CodeArts	Regiões específicas	√	x	x	√	√
CodeArts Req	Regiões específicas	√	√	x	√	x
CloudIDE	Specific regions	√	√	x	√	x

Suporte ao usuário

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
My Account	Regiões específicas	√	x	x	√	x
Billing Center	Regiões específicas	√	x	x	√	x

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Resource Center	Regiões específicas	√	x	x	√	x
Enterprise Project Management Service (EPS)	Regiões globais	√	√	x	√	x
Service Tickets	Regiões globais	√	√	x	x	x
ICP License Service	Regiões globais	√	x	x	x	x
Professional Services	Regiões globais	√	x	x	√	x

Outros

Serviço	Escopo	Console	API	Agência	Política	Projeto empresarial
Message Center	Regiões específicas	√	x	x	√	x

6 Permissões

Se você precisar atribuir permissões diferentes para o IAM aos funcionários em sua organização, o IAM é uma boa opção para o gerenciamento de permissões refinado. O IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a proteger o acesso aos seus recursos da Huawei Cloud.

Com o IAM, você pode criar usuários do IAM em sua conta e atribuir permissões a esses usuários para controlar seu acesso a recursos específicos. Por exemplo, você pode conceder permissões para permitir que determinados planejadores de projetos em sua empresa visualizem dados do IAM, mas não permitir que eles realizem operações de alto risco, por exemplo, excluir usuários e projetos do IAM. Para obter todas as permissões dos serviços suportados pelo IAM, consulte **Permissões definidas pelo sistema**.

Permissões do IAM

Os novos usuários do IAM não têm nenhuma permissão atribuída por padrão. Primeiro você precisa adicioná-los a um ou mais grupos e anexar políticas ou funções a esses grupos. Em seguida, os usuários herdam permissões dos grupos e podem executar operações especificadas em serviços de nuvem com base nas permissões atribuídas a eles.

O IAM é um serviço global implementado em todas as regiões. Quando você define o escopo de autorização como **Global services**, os usuários têm permissão para acessar o IAM em todas as regiões.

Você pode conceder permissões usando funções e políticas.

- Funções: uma estratégia de autorização de alta granularidade fornecida pelo IAM para atribuir permissões com base nas responsabilidades de trabalho dos usuários. Apenas um número limitado de funções em nível de serviço está disponível para autorização. Os serviços de nuvem dependem uns dos outros. Ao conceder permissões usando funções, você também precisa anexar quaisquer dependências de função existentes. As funções não são ideais para autorização refinada e acesso de privilégio mínimo.
- Políticas: uma estratégia de autorização refinada que define as permissões necessárias para realizar operações em recursos específicos de nuvem sob determinadas condições. Esse tipo de autorização é mais flexível e é ideal para acesso de privilégio mínimo. Por exemplo, você pode conceder permissão somente aos usuários para gerenciar ECSs de um determinado tipo. A maioria das políticas refinadas contém permissões para APIs específicas, e as permissões são definidas usando ações da API. Para as ações de API suportadas pelo IAM, consulte **Permissões e ações suportadas**.

Tabela 6-1 lista todas as permissões definidas pelo sistema para o IAM.

Tabela 6-1 Permissões definidas pelo sistema para o IAM

Nome da função/política	Descrição	Tipo	Conteúdo
FullAccess	Permissões completas para todos os serviços que suportam autorização baseada em política. Os usuários com essas permissões podem executar operações em todos os serviços.	Política definida pelo sistema	**Conteúdo da política FullAccess**
IAM ReadOnlyAccess	Permissões somente leitura para o IAM. Os usuários com essas permissões só podem visualizar os dados do IAM.	Política definida pelo sistema	**Conteúdo da política IAM ReadOnlyAccess**
Security Administrator	Administrador do IAM com permissões completas, incluindo permissões para criar e excluir usuários do IAM.	Função definida pelo sistema	**Conteúdo da função Security Administrator**
Agent Operator	Operador de IAM (parte delegada) com permissões para alternar funções e acessar recursos de uma parte delegante.	Função definida pelo sistema	**Conteúdo da função Agent Operator**
Tenant Guest	Permissões somente leitura para todos os serviços, exceto o IAM.	Política definida pelo sistema	**Conteúdo da função Tenant Guest**
Tenant Administrator	Permissões de administrador para todos os serviços, exceto o IAM.	Política definida pelo sistema	**Conteúdo da função Tenant Administrator**

Tabela 6-2 lista as operações comuns suportadas por permissões definidas pelo sistema para o IAM.

NOTA

Tenant Guest e **Tenant Administrator** são funções básicas fornecidas pelo IAM e não contêm permissões específicas para o IAM. Portanto, as duas funções não estão listadas na tabela a seguir.

Tabela 6-2 Operações comuns suportadas por permissões definidas pelo sistema

Operação	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Criação de usuários do IAM	Suportada	Não suportada	Suportada	Não suportada
Consulta de detalhes do usuário do IAM	Suportada	Não suportada	Suportada	Suportada
Modificação de informações do usuário do IAM	Suportada	Não suportada	Suportada	Não suportada
Consulta de configurações de segurança de usuários do IAM	Suportada	Não suportada	Suportada	Suportada
Modificação das configurações de segurança de usuários do IAM	Suportada	Não suportada	Suportada	Não suportada
Exclusão de usuários do IAM	Suportada	Não suportada	Suportada	Não suportada
Criação de grupos de usuários	Suportada	Não suportada	Suportada	Não suportada
Consulta de detalhes do grupo de usuários	Suportada	Não suportada	Suportada	Suportada
Modificação de informações do grupo de usuários	Suportada	Não suportada	Suportada	Não suportada

Operação	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Adição de usuários a grupos de usuários	Suportada	Não suportada	Suportada	Não suportada
Remoção de usuários de grupos de usuários	Suportada	Não suportada	Suportada	Não suportada
Exclusão de grupos de usuários	Suportada	Não suportada	Suportada	Não suportada
Atribuição de permissões a grupos de usuários	Suportada	Não suportada	Suportada	Não suportada
Remoção de permissões de grupos de usuários	Suportada	Não suportada	Suportada	Não suportada
Criação de políticas personalizadas	Suportada	Não suportada	Suportada	Não suportada
Modificação de políticas personalizadas	Suportada	Não suportada	Suportada	Não suportada
Exclusão de políticas personalizadas	Suportada	Não suportada	Suportada	Não suportada
Consulta de detalhes da permissão	Suportada	Não suportada	Suportada	Suportada
Criação de agências	Suportada	Não suportada	Suportada	Não suportada
Consulta de agências	Suportada	Não suportada	Suportada	Suportada
Modificação de agências	Suportada	Não suportada	Suportada	Não suportada
Mudança de funções	Não suportada	Suportada	Suportada	Não suportada

Operação	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Exclusão de agências	Suportada	Não suportada	Suportada	Não suportada
Concessão de permissões a agências	Suportada	Não suportada	Suportada	Não suportada
Remoção de permissões de agências	Suportada	Não suportada	Suportada	Não suportada
Criação de projetos	Suportada	Não suportada	Suportada	Não suportada
Consulta de projetos	Suportada	Não suportada	Suportada	Suportada
Modificação de projetos	Suportada	Não suportada	Suportada	Não suportada
Exclusão de projetos	Suportada	Não suportada	Suportada	Não suportada
Criação de provedores de identidade	Suportada	Não suportada	Suportada	Não suportada
Importação de arquivos de metadados	Suportada	Não suportada	Suportada	Não suportada
Consulta de arquivos de metadados	Suportada	Não suportada	Suportada	Suportada
Consulta de provedores de identidade	Suportada	Não suportada	Suportada	Suportada
Consulta de protocolos	Suportada	Não suportada	Suportada	Suportada
Consulta de mapeamentos	Suportada	Não suportada	Suportada	Suportada
Atualização de provedores de identidade	Suportada	Não suportada	Suportada	Não suportada
Atualização de protocolos	Suportada	Não suportada	Suportada	Não suportada

Operação	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Atualização de mapeamentos	Suportada	Não suportada	Suportada	Não suportada
Exclusão de provedores de identidade	Suportada	Não suportada	Suportada	Não suportada
Exclusão de protocolos	Suportada	Não suportada	Suportada	Não suportada
Exclusão de mapeamentos	Suportada	Não suportada	Suportada	Não suportada
Consulta de cotas	Suportada	Não suportada	Suportada	Não suportada

O gerenciamento de chaves de acesso está desativado por padrão.Quando o **gerenciamento de chaves de acesso** está ativado, somente os administradores podem gerenciar as chaves de acesso. Se os usuários do IAM precisarem criar, ativar, desativar ou excluir suas próprias chaves de acesso, eles deverão pedir ao administrador para **desativar o gerenciamento de chaves de acesso**.

Se um usuário do IAM quiser gerenciar as chaves de acesso de outros usuários do IAM, consulte **Tabela 3**. Por exemplo, se o usuário A do IAM quiser criar uma chave de acesso para o usuário B do IAM, o usuário A do IAM deve ter a permissão Security Administrator ou FullAccess.

Tabela 6-3 Operações da chave de acesso suportadas por políticas ou funções definidas pelo sistema

Operação	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Criação de chaves de acesso (para outros usuários do IAM)	Suportada	Não suportada	Suportada	Não suportada
Consulta de chaves de acesso (de outros usuários do IAM)	Suportada	Não suportada	Suportada	Suportada

Operação	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Modificação de chaves de acesso (para outros usuários do IAM)	Suportada	Não suportada	Suportada	Não suportada
Exclusão de chaves de acesso (para outros usuários do IAM)	Suportada	Não suportada	Suportada	Não suportada

Conteúdo da política FullAccess

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

Conteúdo da política IAM ReadOnlyAccess

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

Conteúdo da função Security Administrator

```
{
    "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"
        }
    ]
}
```

Conteúdo da função Agent Operator

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

Conteúdo da função Tenant Guest

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

Conteúdo da função Tenant Administrator

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



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


7 Segurança

7.1 Responsabilidades compartilhadas

Huawei garante que seu compromisso com a segurança cibernética nunca será superado pela consideração de interesses comerciais. Para lidar com os desafios emergentes de segurança na nuvem e ameaças e ataques à segurança na nuvem, a Huawei Cloud constrói um sistema abrangente de garantia de segurança de serviços em nuvem para diferentes regiões e indústrias com base nas vantagens exclusivas de software e hardware da Huawei, leis, regulamentos, padrões da indústria e ecossistema de segurança.

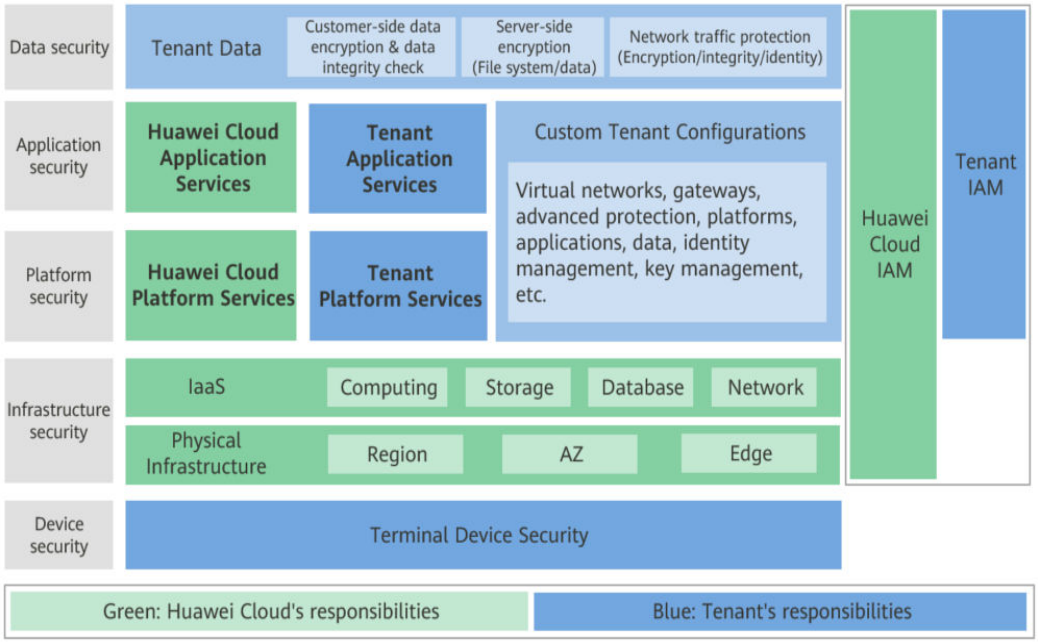
Figura 7-1 ilustra as responsabilidades partilhadas pela Huawei Cloud e pelos usuários.

- **Huawei Cloud**: garante a segurança dos serviços de nuvem e fornece nuvens seguras. As responsabilidades de segurança da Huawei Cloud incluem garantir a segurança de nossos serviços de IaaS, PaaS e SaaS, bem como os ambientes físicos dos data centers da Huawei Cloud onde nossos serviços de IaaS, PaaS e SaaS operam. A Huawei Cloud é responsável não apenas pelas funções de segurança e pelo desempenho de nossa infraestrutura, serviços de nuvem e tecnologias, mas também pela segurança geral de O&M na nuvem e, no sentido mais amplo, pela certificação de segurança de nossa infraestrutura e serviços.
- **Locatário**: usa a nuvem com segurança. Os locatários da Huawei Cloud são responsáveis pelo gerenciamento seguro e eficaz das configurações personalizadas dos serviços em nuvem, incluindo IaaS, PaaS e SaaS. Isso inclui, mas não se limita a, redes virtuais, o SO de hosts e convidados de máquinas virtuais, firewalls virtuais, API Gateway, serviços avançados de segurança, todos os tipos de serviços em nuvem, dados de locatários, contas de identidade e gerenciamento de chaves.

O livro branco de segurança da Huawei Cloud elabora as ideias e medidas para a construção da segurança da Huawei Cloud, incluindo estratégias de segurança na nuvem, o

modelo de responsabilidade compartilhada, conformidade e privacidade, organizações e pessoal de segurança, segurança de infraestrutura, serviço e segurança de locatários, segurança de engenharia, segurança de O&M e segurança do ecossistema.

Figura 7-1 Modelo de responsabilidade de segurança compartilhada da Huawei Cloud



7.2 Autenticação e controle de acesso

7.2.1 Autenticação de identidade

O serviço IAM exige que o solicitante de acesso apresente a credencial de identidade e verifica a validade da identidade. Além disso, o serviço IAM fornece proteção de logon e políticas de verificação para fortalecer a segurança da autenticação de identidade.

Credenciais de identidade e sua segurança

O IAM pode ser acessado usando contas e usuários do IAM. Ambos suportam autenticação de identidade usando nomes de usuário, senhas, chaves de acesso e chaves de acesso temporárias. O IAM implementa o design de segurança para cada credencial de identidade para proteger os dados do usuário e permitir que os usuários acessem o IAM com mais segurança. Para mais detalhes, consulte **Tabela 7-1**.

Tabela 7-1 Credenciais de identidade do IAM e design de segurança

Credencial de acesso	Descrição de segurança	Referência
Nome do usuário e senha	Você pode configurar o tipo de caractere e o comprimento mínimo de uma chave de usuário, conforme necessário. Você pode igualmente configurar a política do período de validade da senha e a política de período mínimo de validade da senha.	**Política de senha**
Chave de acesso	O AK é usado em conjunto com a SK para assinar solicitações criptograficamente, garantindo que as solicitações sejam secretas, completas e corretas.	**Chaves de acesso**
Chave de acesso temporária	Além do recurso de chave de acesso, uma chave de acesso temporária tem um período de validade que pode ser personalizado. Se o período de validade expirar, a chave de acesso temporária se tornará inválida e você terá que obter uma nova.	**Chave de acesso temporária (para usuários federados)**

Políticas de proteção e autenticação de logon

Conforme descrito em **Tabela 7-2**, além de exigir que os usuários mostrem credenciais e verifiquem sua validade durante o logon, o IAM também fornece proteção de logon e suporta políticas de verificação de logon para evitar que as informações do usuário sejam roubadas.

Tabela 7-2 Políticas de proteção e autenticação de logon

Método de proteção de logon	Descrição	Funções
Proteção de logon	Além de inserir o nome de usuário e a senha na página de logon (autenticação pela primeira vez), você precisa inserir um código de verificação na página **Login Verification** (autenticação pela segunda vez). Verifique se há suporte para números de celular, endereços de e-mail e dispositivos de MFA virtual. Para obter detalhes, consulte **Autenticação MFA**.	**Proteção de logon**
Política de autenticação de logon	O IAM oferece suporte às seguintes políticas de autenticação de logon: Política de **tempo limite da sessão**: se um usuário não fizer logon no sistema dentro de um período especificado, ele precisará fazer logon novamente. Política de **bloqueio de conta**: se o número de falhas de logon exceder o limite, a conta será bloqueada. Política de **desativação de conta**: se um usuário não fizer logon no sistema por um longo tempo, a conta será desativada. Exibição de **informações de logon recentes**: permite que os usuários visualizem o último horário de logon.	**Política de autenticação de logon**

7.2.2 Configuração do controle de acesso

O IAM usa políticas de autorização refinadas e ACLs para controlar o acesso.

Tabela 7-3 Controle de acesso ao IAM

Política de acesso	Descrição	Referência
Política de autorização refinada do IAM	As permissões de serviço do IAM são divididas em funções ou políticas refinadas. As funções e as políticas definem as operações de usuário permitidas ou rejeitadas pelo IAM. Por exemplo, se um usuário ou grupo de usuários tiver a permissão IAM ReadOnlyAccess, o usuário ou grupo de usuários terá apenas a permissão somente leitura nos dados de serviço do IAM. O IAM também oferece suporte a **políticas personalizadas** para atribuir permissões de serviço do IAM.	**Permissões do IAM**
ACL	Com a ACL, você pode definir políticas de controle de acesso para permitir que os usuários façam logon no console do IAM ou abram APIs somente a partir de intervalos de endereços IP, segmentos de rede e pontos de extremidade da VPC especificados.	**ACL**

7.3 Proteção de dados

7.3.1 Lado do IAM

Para garantir que seus dados pessoais, como nome de usuário, senha e número de telefone celular, não serão obtidos por entidades ou indivíduos não autorizados ou não autenticados, o IAM criptografa seus dados durante o armazenamento e a transmissão para evitar vazamento de dados.

Dados pessoais

Tabela 7-4 lista os dados pessoais gerados ou coletados pelo IAM.

Tabela 7-4 Dados pessoais

Tipo	Origem	Usado para	Modificável	Obrigatório
Nome de usuário	● Inserido quando você cria um usuário no console de gerenciamento. ● Inserido quando você chama uma API.	● Identificação de identidade do usuário ● Autenticação de identidade durante o acesso ao console ou chamadas de API	Sim (Os administradores podem chamar a API para alterar o nome de usuário.)	Sim Os nomes de usuário são usados para identificar usuários.
Senha	● Inserido quando você cria um usuário, modifica as credenciais do usuário ou redefine a senha no console de gerenciamento. ● Inserido quando você chama uma API.	Autenticação de identidade durante o acesso ao console ou chamadas de API	Sim	Não Você também pode escolher a autenticação de AK/SK.
Endereço de e-mail	Inserido quando você cria um usuário, modifica credenciais de usuário ou altera o endereço de e-mail no console de gerenciamento.	● Identificação de identidade do usuário ● Autenticação de identidade durante o acesso ao console ● Receber mensagens	Sim	Não
Número de celular	Inserido quando você cria um usuário, modifica credenciais de usuário ou altera o número de celular no console de gerenciamento.	● Identificação de identidade do usuário ● Autenticação de identidade durante o acesso ao console ● Receber mensagens	Sim	Não

Tipo	Origem	Usado para	Modificável	Obrigatório
AK/SK	Exibido na área **Security Settings** > **Access Keys** de um usuário específico no console do IAM ou na página **My Credentials** > **Access Keys**.	Autenticação de identidade durante chamadas de API	Não AK/SK não pode ser modificada, mas pode ser excluída e criada novamente.	Não AK/SK é usada para assinar as solicitações enviadas para chamar APIs.

Segurança de armazenamento de dados

O IAM usa algoritmos de criptografia para criptografar os dados do usuário antes de armazená-los.

- Nomes de usuário e AKs: dados não confidenciais, que são armazenados em texto não criptografado.
- Senha: a senha é criptografada usando o algoritmo SHA512 salgado.
- Endereço de e-mail, número de celular e SK: uso do algoritmo AES para criptografá-los e armazená-los.

Segurança de transmissão de dados

Os dados confidenciais (incluindo senhas) dos usuários são criptografados usando o TLS 1.2 durante a transmissão. Todas as APIs do IAM oferecem suporte a HTTPS para criptografar dados durante a transmissão.

7.3.2 Lado do locatário

As **responsabilidades compartilhadas** se aplicam à proteção de dados no IAM da Huawei Cloud. Como mencionado, o IAM é responsável pela segurança do próprio serviço e fornece um mecanismo seguro de proteção de dados. Os locatários são responsáveis pelo uso seguro dos serviços de IAM, incluindo a configuração de parâmetros de segurança e a divisão e concessão de permissões pelas empresas.

Para fins de proteção de dados, recomendamos que você use o IAM de maneira mais padrão, consultando **Recomendações para o uso do IAM**.

7.4 Resiliência

Os data centers da Huawei Cloud são implementados em todo o mundo. Todos os data centers estão funcionando corretamente. Data centers em duas cidades são implementados como centro de recuperação de desastres um para o outro. Se um data center na cidade A estiver inativo, o data center na cidade B assumirá automaticamente o trabalho e atenderá suas aplicações e dados em conformidade com os regulamentos para garantir a continuidade do serviço. Para minimizar as interrupções de serviço causadas por falhas de hardware, desastres

naturais ou outros eventos desastrosos, a Huawei Cloud fornece um plano de DR para todos os data centers:

Como um serviço básico de autenticação de identidade, o IAM da Huawei Cloud foi implementado em várias zonas para fornecer aos usuários globais maior disponibilidade, tolerância a falhas e escalabilidade.

7.5 Auditoria e monitoramento

O Cloud Trace Service (CTS) registra as operações realizadas em recursos de nuvem em sua conta. Os logs de operações podem ser usados para realizar análises de segurança, rastrear alterações de recursos, realizar auditorias de conformidade e localizar falhas.

Para obter detalhes sobre as operações do IAM que podem ser registradas pelo CTS, consulte "Operações do IAM que podem ser registradas pelo CTS" em **Ativação do CTS**. Depois que você ativa o CTS e cria e configura um rastreador, o CTS começa a registrar operações para auditoria. Para obter detalhes, consulte **Ativação do CTS**. Depois que o CTS estiver ativado, você poderá **visualizar os logs de auditoria do IAM**. O CTS armazena logs de operação dos últimos sete dias.

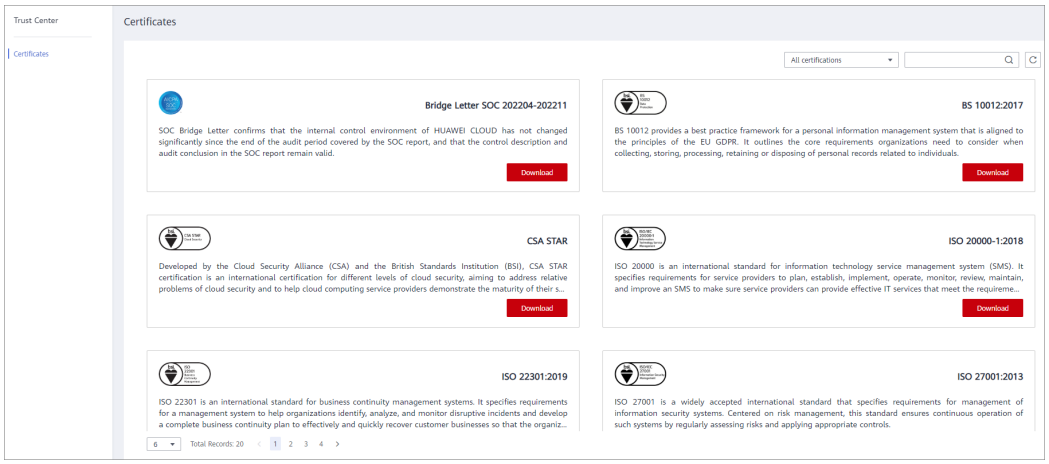
O CTS permite que você **configure notificações de eventos importantes**. Você pode adicionar operações sensíveis e de alto risco relacionadas ao IAM como operações-chave à lista de monitoramento em tempo real do CTS para monitoramento e rastreamento. Se uma operação-chave na lista de monitoramento for acionada quando um usuário usar o serviço IAM, o CTS registrará o log de operação e enviará uma notificação ao assinante relacionado em tempo real.

7.6 Certificados

Certificados de conformidade

Os serviços e plataformas da Huawei Cloud obtiveram várias certificações de segurança e de conformidade das organizações autorizadas, como a Organização Internacional de Normalização (ISO).

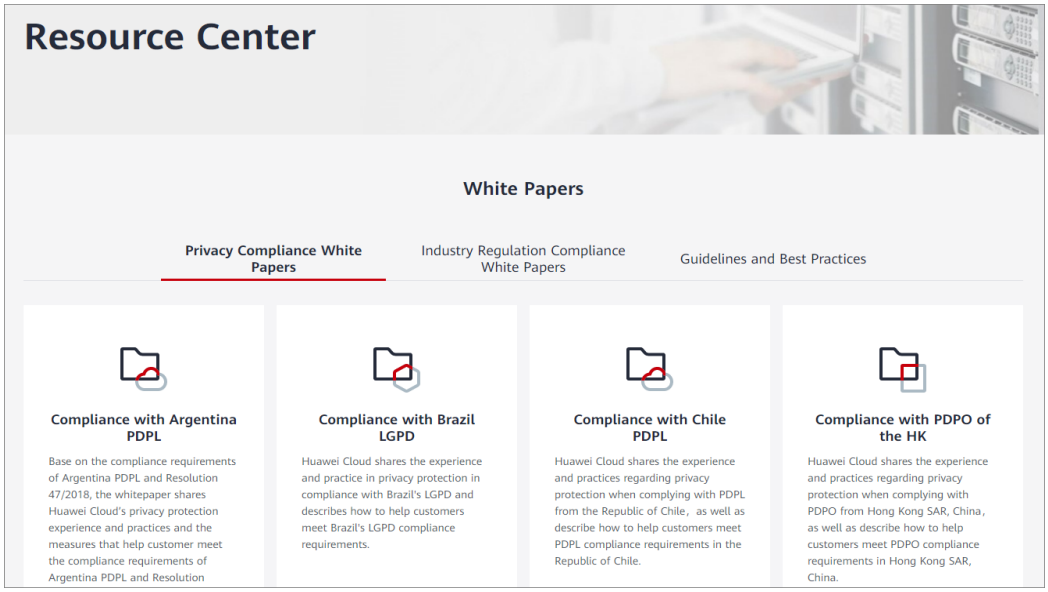
Figura 7-2 Download de certificados de conformidade



Central de recursos

A Huawei Cloud também fornece os seguintes recursos para ajudar os usuários a atender aos requisitos de conformidade. Para obter detalhes, consulte **Central de recursos**.

Figura 7-3 Central de recursos



8 Observações e restrições

A tabela a seguir lista as cotas de vários recursos no IAM. Para obter detalhes, consulte **Como aumentar minha cota?**

Categoria	Item	Cota	Ajustável
Usuário	Usuários do IAM	50	Sim
	Caracteres permitidos em um nome de usuário	32	Não
	Grupos aos quais um usuário pode ser adicionado	10	Não
	Pares AK/SK que um usuário pode criar	2	Não
	Dispositivos de MFA virtual que podem ser vinculados a um usuário	1	Não
	Permissões (incluindo permissões definidas pelo sistema e políticas personalizadas) que podem ser atribuídas a um usuário para projetos empresariais	500	Sim
Grupo de usuários	Grupos de usuários	20	Sim

Categoria	Item	Cota	Ajustável
	Caracteres permitidos em um nome de grupo de usuários	128	Não
	Usuários que podem ser adicionados a um grupo de usuários	Usuários do IAM que foram criados usando sua conta	Não
	Permissões (incluindo permissões definidas pelo sistema e políticas personalizadas) que podem ser atribuídas a um grupo de usuários para projetos do IAM	200	Sim
	Permissões (incluindo permissões definidas pelo sistema e políticas personalizadas) que podem ser atribuídas a um grupo de usuários para projetos empresariais	500	Sim
Projeto	Subprojetos em cada região	10	Sim
Política	Caracteres permitidos em um nome de política	128	Não
Política personalizada	Políticas personalizadas	200	Sim
	Caracteres por política	6.144	Não
	Declarações por política	Ilimitada	Não
	Ações por declaração	Ilimitada	Não

Categoria	Item	Cota	Ajustável
	Recursos por declaração	Ilimitada	Não
	Condições por declaração	Ilimitada	Não
Agência	Agências	50	Sim
	Caracteres permitidos em um nome de agência	64	Não
	Permissões (incluindo permissões definidas pelo sistema e políticas personalizadas) que podem ser atribuídas a uma agência	200	Sim
Provedor de identidade	Quantidade	10	Sim
	Caracteres que podem estar contidos em um nome de provedor de identidade	64	Não
	Regras de mapeamento de todos os provedores de identidade em uma conta	10	Sim

9 Histórico de alterações

Tabela 9-1 Histórico de alterações

Data	Descrição
10/11/2022	Esta edição é o 18º lançamento oficial, que incorpora a seguinte alteração: Adição de introdução aos recursos de segurança do IAM em **7 Segurança**.
01/12/2021	Esta edição é o 17º lançamento oficial, que incorpora a seguinte alteração: Adição da cota de regra de conversão de identidade em **8 Observações e restrições**.
23/11/2021	Esta edição é o 16º lançamento oficial, que incorpora a seguinte alteração: Adição da descrição de projetos empresariais em **5 Serviços de nuvem com suporte**.
25/04/2021	Esta edição é o 15º lançamento oficial, que incorpora a seguinte alteração: Adição de cotas de permissão em **8 Observações e restrições**.
30/12/2020	Esta edição é o 14º lançamento oficial, que incorpora a seguinte alteração: Atualização das capturas de tela em **3 Conceitos básicos** com base na alteração no método de logon.
30/11/2020	Esta edição é o 13º lançamento oficial, que incorpora a seguinte alteração: Atualização da descrição com base nas alterações na página de configuração de segurança.

Data	Descrição
27/10/2020	Esta edição é o 12º lançamento oficial, que incorpora a seguinte alteração: Atualização das capturas de tela em **3 Conceitos básicos** com base na alteração no método de logon.
30/09/2020	Esta edição é o 11º lançamento oficial, que incorpora a seguinte alteração: Adição da seção **6 Permissões**.
11/06/2020	Esta edição é o 10º lançamento oficial, que incorpora a seguinte alteração: Alteração do número máximo de grupos de usuários aos quais um usuário pode ser adicionado para **10** em **8 Observações e restrições**.
08/06/2020	Esta edição é o 9º lançamento oficial, que incorpora a seguinte alteração: Adição de descrições sobre a HUAWEI ID em **3 Conceitos básicos** e atualização das capturas de tela da página de logon.
19/01/2020	Esta edição é o 8º lançamento oficial, que incorpora as seguintes alterações: ● Otimização da descrição das permissões em **3 Conceitos básicos**. ● Adição do limite de subprojetos em uma região em **8 Observações e restrições**.
20/11/2019	Esta edição é o 7º lançamento oficial, que incorpora a seguinte alteração: Aumento da cota de política personalizada para 200 em **8 Observações e restrições**.
05/06/2019	Esta edição é o 6º lançamento oficial. Modificação de descrições nos capítulos **2 O que é o IAM?**, **3 Conceitos básicos** e **4 Funções**.
05/03/2019	Esta edição é o 5º lançamento oficial. Adição de capítulo **8 Observações e restrições**.
20/02/2019	Esta edição é o 4º lançamento oficial. Adição de capítulo **3 Conceitos básicos**.
15/01/2019	Esta edição é o 3º lançamento oficial. Adição de capítulo **5 Serviços de nuvem com suporte**.
10/08/2018	Esta edição é o 2º lançamento oficial, que incorpora a seguinte alteração: Adição de "Proteção de dados pessoais".
30/03/2018	Esta edição é o 1º lançamento oficial.

