Nuvem Privada Virtual

Visão geral de serviço

Edição 01

Data 2024-09-14

HUAWEI CLOUD COMPUTING 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, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem 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 ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

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 Cloud Computing Technologies Co., Ltd.

Endereço: Huawei Cloud Data Center, Rua Jiaoxinggong
Avenida Qianzhong
Novo Distrito de Gui'an
Guizhou 550029
República Popular da China

Site: https://www.huaweicloud.com/intl/pt-br/

Índice

1 O que é Virtual Private Cloud?

Visão geral

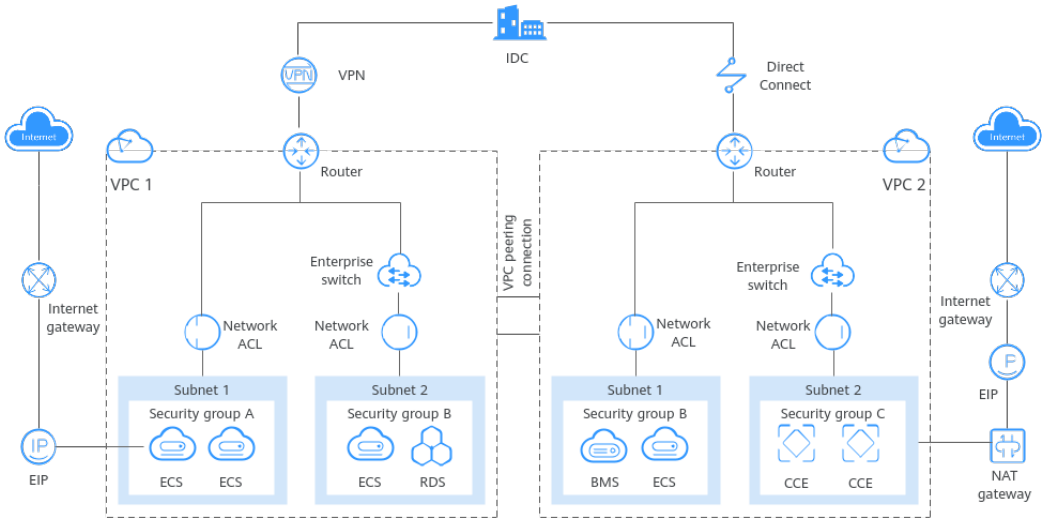
O serviço Virtual Private Cloud (VPC) permite provisionar redes virtuais logicamente isoladas para recursos de nuvem, como servidores de nuvem, contêineres e bancos de dados. Você pode criar sub-redes personalizadas, grupos de segurança, network ACLs e atribuir EIPs e larguras de banda. Com a Direct Connect ou a Virtual Private Network (VPN), você pode conectar suas VPCs a um data center local.

O serviço VPC usa tecnologias de virtualização de rede, como redundância de links, clusters de gateway distribuídos e implementação em várias AZs, para garantir a segurança, a estabilidade e a disponibilidade da rede.

Arquitetura do produto

A arquitetura do produto consiste em componentes da VPC, recursos de segurança e opções de conectividade da VPC.

Figura 1-1 Arquitetura



Visão geral da tabela de rotas

Componentes da VPC

Cada VPC consiste em um bloco CIDR privado, tabelas de rotas e pelo menos uma sub-rede.

- Bloco CIDR privado: ao criar uma VPC, é necessário especificar o bloco CIDR privado utilizado pela VPC. O serviço VPC é compatível com seguintes blocos CIDR: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 e 192.168.0.0 – 192.168.255.255
- Sub-redes: recursos em nuvem (como servidores e bancos de dados em nuvem) devem ser implementados em sub-redes. Depois de criar uma VPC, você pode dividi-la em uma ou mais sub-redes. Cada sub-rede deve estar dentro da VPC. Para mais informações, consulte **Sub-rede**.
- Tabelas de rotas: quando você cria uma VPC, o sistema gera automaticamente uma tabela de rotas predefinida. A tabela de rotas garante que todas as sub-redes na mesma VPC possam se comunicar entre si. Se as rotas na tabela de rotas padrão não puderem atender aos requisitos da aplicação (por exemplo, se houver um ECS sem um endereço IP elástico (EIP) vinculado que precisa acessar a Internet), você pode criar uma tabela de rotas personalizada. Para obter mais informações, consulte **Visão geral da tabela de rotas**.

Recursos de segurança

Grupos de segurança e network ACLs garantem a segurança dos recursos de nuvem implantados em uma VPC. Um grupo de segurança atua como um firewall virtual para fornecer regras de acesso para instâncias que têm os mesmos requisitos de segurança e são mutuamente confiáveis em uma VPC. Para mais informações, consulte **Visão geral de grupo de segurança**. Uma network ACL pode ser associada a sub-redes que tenham os mesmos requisitos de controle de acesso. Você pode adicionar regras de entrada e saída para controlar com precisão o tráfego de entrada e saída no nível da sub-rede. Para mais informações, consulte **Visão geral de Network ACL**.

Conectividade de VPC

Huawei Cloud oferece várias opções de conectividade VPC para atender a diferentes requisitos. Para obter detalhes, consulte **Cenários de aplicação**.

- O emparelhamento de VPC permite que duas VPCs na mesma região se comuniquem usando endereços IP privados.
- Elastic IP ou NAT Gateway permite que os ECSs em uma VPC se comuniquem com a Internet.
- Virtual Private Network (VPN), Cloud Connect ou Direct Connect podem conectar uma VPC ao seu data center.

Acessar o serviço VPC

Você pode acessar o serviço VPC por meio do console de gerenciamento ou usando APIs baseadas em HTTPS.

- Console de gerenciamento

  Você pode usar o console para executar operações diretamente em recursos da VPC. Para acessar o serviço da VPC, faça logon no **console de gerenciamento** e selecione **Virtual Private Cloud** na página inicial do console.

- API

  Se você precisar integrar a VPC a um sistema de terceiros para desenvolvimento secundário, use as API para acessar o serviço VPC. Para obter detalhes, consulte a **Referência de API daVirtual Private Cloud**.

2 Vantagens do produto

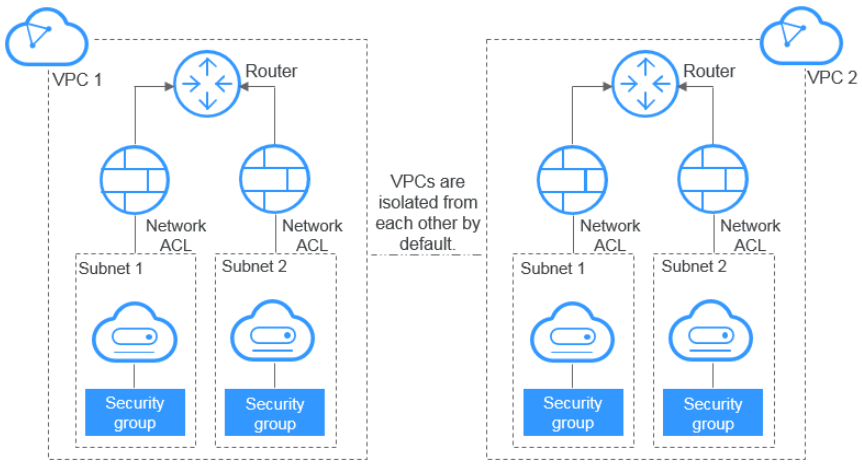
Configuração flexível

Você pode criar VPCs, adicionar sub-redes, especificar intervalos de endereços IP e configurar tabelas DHCP e de rota. Você pode configurar a mesma VPC para ECSs que estão em zonas de disponibilidade (AZs) diferentes.

Seguro e confiável

As VPCs são logicamente isoladas por meio de tecnologias de tunelamento. Por padrão, VPCs diferentes não podem se comunicar entre si. Você pode usar ACL da rede para proteger sub-redes e usar grupos de segurança para proteger ECSs. Elas adicionam camadas adicionais de segurança às suas VPCs, para que sua rede fique segura.

Figura 2-1 Seguro e confiável



Interconectividade sem emenda

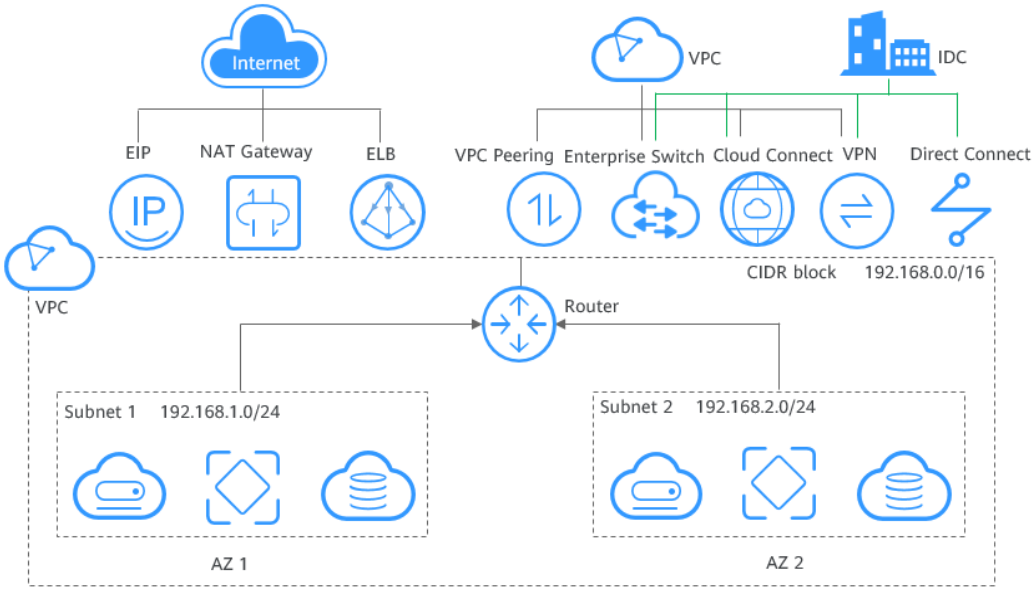
Por padrão, as instâncias em uma VPC não podem acessar a Internet. Você pode usar EIPs, balanceadores de carga, gateways da NAT conexões de VPN e conexões Direct Connect para habilitar o acesso de ou para a Internet.

Por padrão, diferentes VPCs não podem se comunicar entre si. Você pode criar uma conexão de emparelhamento de VPC para permitir que as instâncias nas duas VPCs na mesma região se comuniquem usando endereços IP privados.

Você pode usar um gateway de conexão da Camada 2 (L2CG) fornecido pelo nosso serviço Enterprise Switch para estabelecer comunicação de rede entre a nuvem e as redes locais e migrar o data center ou os serviços de nuvem privada para a nuvem sem alterar as sub-redes.

Várias opções de conectividade estão disponíveis para atender a diversos requisitos de serviço para a nuvem, permitindo que você implemente aplicativos empresariais com facilidade e reduza os custos de operação e manutenção (O&M) de TI corporativa.

Figura 2-2 Interconectividade



Acesso de alta velocidade

O BGP dinâmico é usado para fornecer acesso a várias redes de operadoras. Você pode estabelecer mais de 20 conexões de BGP dinâmico para diferentes operadoras. Conexões de BGP dinâmico permitem failovers em tempo real com base em protocolos de roteamento predefinidos, garantindo alta estabilidade de rede, baixa latência de rede e acesso fácil a serviços na nuvem.

Comparação de vantagens

Tabela 2-1 lista as vantagens de uma VPC em relação a uma IDC tradicional.

Tabela 2-1 Comparação entre uma VPC e um IDC tradicional

Item	VPC	IDC tradicional
Ciclo de implementação	● Você não precisa executar implantação de engenharia complexa, incluindo planejamento de engenharia e cabeamento. ● Você pode determinar suas redes, sub-redes e rotas na Huawei Cloud com base nos requisitos de serviço.	Você precisa configurar redes e realizar testes. Todo o processo leva muito tempo e requer suporte técnico profissional.
Custo total	Huawei Cloud oferece modos de cobrança flexíveis para serviços de rede. Você pode selecionar o que melhor se adapta às suas necessidades de negócios. Não há custos iniciais e custos de O&M de rede, reduzindo o custo total de propriedade (TCO).	Você precisa investir pesadamente em salas de equipamentos, fornecimento de energia, construção e materiais de hardware. Você também precisa de equipes profissionais de O&M para garantir a segurança da rede. Os custos de gerenciamento de ativos aumentam com qualquer mudança nos requisitos de negócios.
Flexibilidade	Huawei Cloud oferece uma variedade de serviços de rede para você escolher. Se você precisar de mais recursos de rede (por exemplo, se precisar de mais largura de banda), poderá expandir os recursos rapidamente.	Você precisa cumprir rigorosamente o plano de rede para concluir a implementação do serviço. Se houver alterações em seus requisitos de serviço, é difícil ajustar dinamicamente a rede.
Segurança	As VPCs são logicamente isoladas umas das outras. Você pode usar recursos de segurança, como network ACLs e grupos de segurança, e até mesmo serviços de segurança como Advanced Anti-DDoS (AAD) para proteger seus recursos de nuvem.	A rede é insegura e difícil de manter. Você precisa de equipe técnico profissional para garantir a segurança da rede.

3 Cenários de aplicação

Redes dedicadas na nuvem

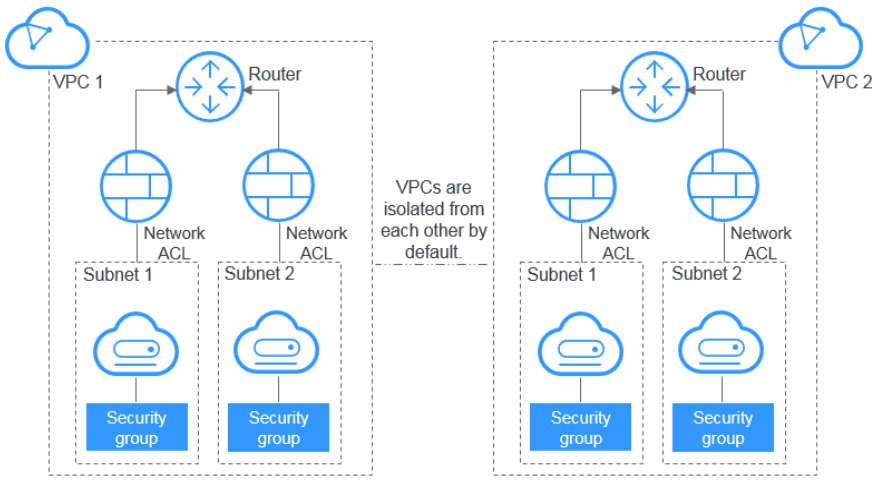
Cenário

Cada VPC representa uma rede privada e é logicamente isolada de outras VPCs. Você pode implementar seu sistema de serviço em uma VPC para que ele tenha um ambiente de rede privada na Huawei Cloud. Se você tiver vários sistemas de serviço, por exemplo, um sistema de produção e um sistema de teste, poderá implementá-los em duas VPCs diferentes para mantê-los isolados. Se você deseja estabelecer comunicação entre esses duas VPCs, pode criar uma conexão de emparelhamento de VPC para vinculá-los

Serviços relacionados

ECS

Figura 3-1 Redes dedicadas na nuvem



Aplicação Web ou hospedagem de sites

Cenário

Você pode hospedar aplicações e sites da Web em uma VPC e usar a VPC como uma rede comum. Com EIPs ou gateways da NAT, você pode conectar ECSs que executam suas

aplicações Web à Internet. Você pode usar balanceadores de carga fornecidos pelo serviço ELB para distribuir o tráfego uniformemente entre vários ECSs.

Os recursos de nuvem em uma VPC podem usar os seguintes serviços de nuvem para se conectar à Internet.

Tabela 3-1 Acessar a Internet

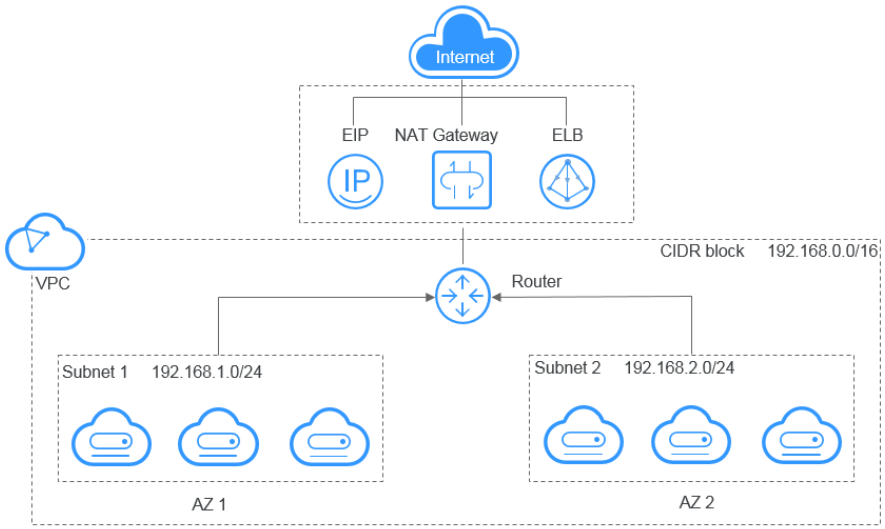
Serviço de nuvem	Cenário de aplicação	Descrição	Operações relacionadas
EIP	Um único ECS acessa a Internet.	Você pode atribuir um EIP e vinculá-lo a um ECS para que o ECS possa acessar a Internet ou fornecer serviços acessíveis a partir da Internet. Você pode desvincular o EIP do ECS para desabilitar o acesso a qualquer momento. Você pode usar largura de banda compartilhada e pacotes de dados compartilhados para simplificar os custos.	**Elastic IP**
NAT Gateway	Vários ECSs compartilham um EIP para acessar a Internet.	Um gateway da NAT oferecem tradução de endereço de rede de origem (SNAT) e tradução de endereço de rede de destino (DNAT). A SNAT permite que vários ECSs na mesma VPC compartilhem EIPs para acessar a Internet. Dessa forma, você pode reduzir os custos de gerenciamento e evitar que os EIPs dos ECSs sejam expostos à Internet. A DNAT usa o encaminhamento de dados em nível de porta. Ela mapeia portas EIP para portas ECS para que os ECSs em uma VPC possam compartilhar o mesmo EIP e largura de banda para fornecer serviços acessíveis pela Internet. No entanto, a DNAT não equilibra o tráfego.	**Uso da SNAT para acessar a Internet** **Uso da DNAT para fornecer serviços acessíveis a partir da Internet**

Serviço de nuvem	Cenário de aplicação	Descrição	Operações relacionadas
ELB	Distribuir uniformemente o tráfego de entrada entre vários ECSs em cenários de alta concorrência, como comércio eletrônico.	Os balanceadores de carga distribuem uniformemente o tráfego entre vários ECSs de back-end (na Camada 4 ou Camada 7). Você pode vincular EIPs a ECSs para permitir o acesso da Internet. O ELB expande os recursos e melhora a disponibilidade de suas aplicações eliminando pontos únicos de falhas.	**O que é Elastic Load Balance?**

Serviços relacionados

ECS, EIP, NAT Gateway e ELB

Figura 3-2 Aplicação Web ou hospedagem de sites



Controle de acesso à aplicação Web

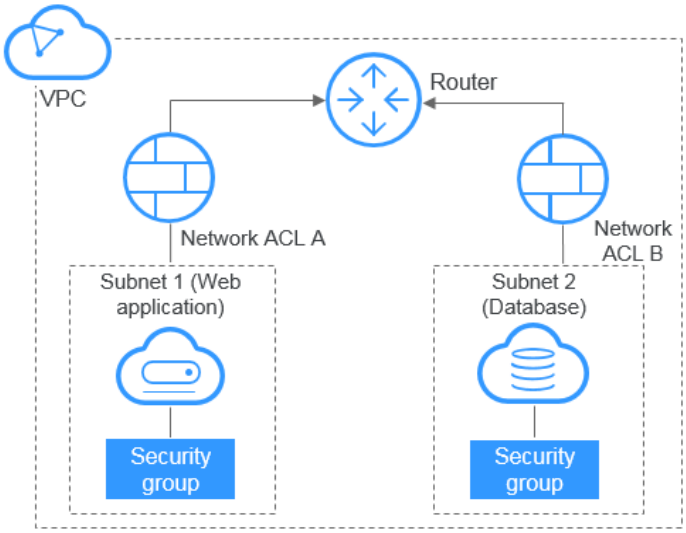
Cenário

Você pode criar uma VPC e grupos de segurança para hospedar aplicações Web de várias camadas em diferentes zonas de segurança. Você pode associar servidores Web e servidores de banco de dados a diferentes grupos de segurança e configurar diferentes regras de controle de acesso para grupos de segurança. Você pode iniciar servidores Web em uma sub-rede acessível ao público. Mas então, para garantir a segurança, você pode executar servidores de banco de dados em sub-redes que não são acessíveis ao público.

Serviços relacionados

ECS

Figura 3-3 Controle de acesso à aplicação Web



Opções de conectividade da VPC

Cenário

Você pode usar os seguintes serviços em nuvem para permitir que duas VPCs se comuniquem entre si.

Tabela 3-2 Conectar-se a VPCs

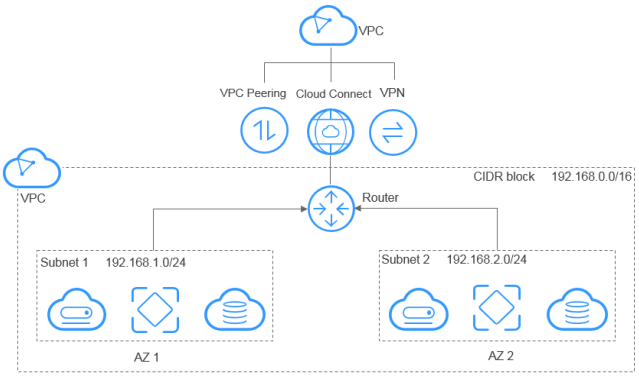
Serviço de nuvem	Cenário de aplicação	Descrição	Operações relacionadas
Emparelhamento de VPC	Conectar VPCs na mesma região.	Você pode solicitar uma conexão de emparelhamento de VPC com outra VPC na sua conta ou em outra conta, mas as duas VPCs devem estar na mesma região. As conexões de emparelhamento de VPC são gratuitas.	**Criação de uma conexão de emparelhamento de VPC com uma outra VPC na sua conta** **Criação de uma conexão de emparelhamento de VPC com uma VPC em outra conta**
Cloud Connect	Conetar VPCs em diferentes regiões.	A Cloud Connect permite conectar duas VPCs na mesma conta ou em contas diferentes, mesmo que estejam em regiões diferentes.	**Comunicação entre VPCs entre regiões**

Serviço de nuvem	Cenário de aplicação	Descrição	Operações relacionadas
VPN	Usar a VPN para conectar VPCs entre regiões a baixo custo.	A VPN usa um túnel de comunicação criptografado para conectar VPCs em diferentes regiões e enviar tráfego pela Internet. É barata, fácil de configurar e fácil de usar. No entanto, a qualidade das conexões de VPN depende da qualidade de suas conexões de Internet.	**Conexão a uma VPC por meio de uma VPN**

Serviços relacionados

ECS, Cloud Connect e VPN

Figura 3-4 Opções de conectividade da VPC



Implementação de nuvem híbrida

Cenário

Se você tiver um data center local e não quiser migrar todos os seus serviços para a nuvem, poderá criar uma nuvem híbrida, que permitirá manter os dados principais em seu data center.

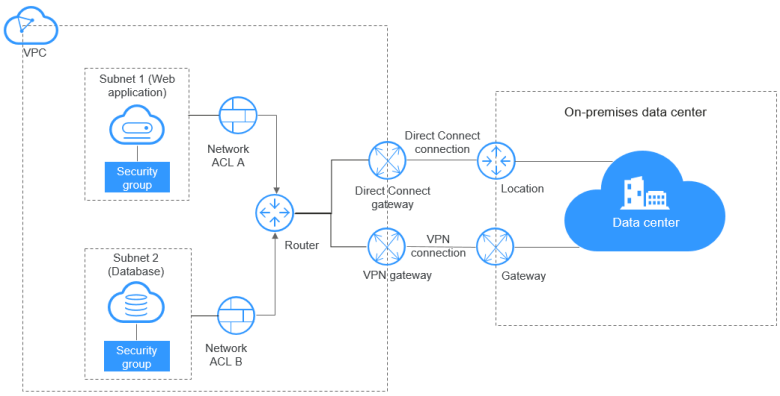
Tabela 3-3 Conetar com um data center local

Serviço de nuvem	Cenário de aplicação	Descrição	Operações relacionadas
VPN	Usar a VPN para conectar uma VPC a um data center local a baixo custo.	A VPN usa um túnel de comunicação criptografado para conectar uma VPC na nuvem a um data center local e enviar tráfego pela Internet. É barata, fácil de configurar e fácil de usar. No entanto, a qualidade das conexões de VPN depende da qualidade de suas conexões de Internet.	**Conexão a uma VPC por meio de uma VPN** **Uso de um Enterprise Switch para permitir que um data center local e uma VPC se comuniquem na camada 2**
Direct Connect	Usar uma conexão física para conectar uma VPC a um data center local.	A Direct Connect fornece conexões físicas entre VPCs e data centers. Possui baixa latência e é muito seguro. A Direct Connect é uma boa escolha se você tiver requisitos rigorosos sobre a qualidade da transmissão da rede.	**Acesso de várias VPCs usando uma conexão** **Uso de um Enterprise Switch para permitir que um data center local e uma VPC se comuniquem na camada 2**

Serviços relacionados

Cloud Connect, ECS, Direct Connect e VPN

Figura 3-5 Implementação de nuvem híbrida



4 Funções

Tabela 4-1 lista funções comuns da VPC.

Antes de usar o serviço VPC, você deve estar familiarizado com os conceitos básicos, como sub-redes, tabelas de rotas, grupos de segurança e EIPs. Isso facilitará a compreensão das funções da VPC.

Tabela 4-1 Funções comuns da VPC

Categoria	Função	Descrição
VPC e sub-rede	VPC	Uma VPC fornece uma rede virtual isolada para seus recursos de nuvem. Você pode configurar e gerenciar a rede de forma flexível. Você pode criar VPCs, modificar informações básicas sobre VPCs, adicionar um bloco CIDR secundário a uma VPC, remover um bloco CIDR secundário de uma VPC, excluir VPCs e exportar a lista de VPCs. Para obter detalhes, consulte **Criação de uma VPC**.
	Sub-rede	Uma sub-rede é um bloco CIDR único com um intervalo de endereços IP na sua VPC. Todos os recursos em uma VPC devem ser implementados em sub-redes. Você pode criar sub-redes, modificar informações de sub-rede e excluir sub-redes. Para obter detalhes, consulte **Criação de uma VPC**.

Categoria	Função	Descrição
	Tabela de rotas	Uma tabela de rotas contém rotas, que determinam para onde o tráfego é direcionado. Quando você cria uma VPC, o sistema gera automaticamente uma tabela de rotas predefinida. A tabela de rotas garante que todas as sub-redes na mesma VPC possam se comunicar entre si. Você também pode adicionar rotas personalizadas para controlar para onde o tráfego é direcionado. Você pode adicionar, consultar, modificar e excluir rotas. Para obter detalhes, consulte **Visão geral de tabela de rotas**.
	Endereço IP virtual	Um endereço IP virtual pode ser compartilhado entre vários ECSs. Você pode configurar endereços IP privados e virtuais para um ECS e pode acessar o ECS por meio de um endereço IP. Um endereço IP virtual tem a mesma capacidade de acesso à rede que um endereço IP privado. Se você precisar de alta disponibilidade, poderá usar endereços IP virtuais porque eles oferecem suporte à alternância de ECS ativo/em espera. Você pode atribuir e liberar endereços IP virtuais, vincular um endereço IP virtual a um EIP ou ECS e acessar um endereço IP virtual por meio de um EIP, uma VPN, Direct Connect ou conexão de emparelhamento de VPC. Para obter detalhes, consulte **Visão geral de endereço IP virtual**.
	Rede de pilha dupla IPv4 e IPv6	A pilha dupla IPv4 e IPv6 permite que seus recursos usem os endereços IPv4 e IPv6 para comunicação de rede privada e pública. Você pode criar uma rede de pilha dupla IPv4/IPv6 ou adicionar uma sub-rede IPv6 a uma VPC para formar uma rede de pilha dupla. Para obter detalhes, consulte **Rede de pilha dupla IPv4 e IPv6**.
	Log de fluxo de VPC	Um log de fluxo de VPC registra informações sobre o tráfego indo e vindo de uma VPC. Os logs de fluxo da VPC ajudam a monitorar o tráfego de rede, analisar ataques à rede e determinar se o grupo de segurança e as regras de network ACL exigem modificação. Você pode criar, visualizar, ativar, desativar e excluir logs de fluxo da VPC. Para obter detalhes, consulte **Visão geral de log de fluxo da VPC**.

Categoria	Função	Descrição
Controle de acesso	Grupo de segurança	Um grupo de segurança é uma coleção de regras de controle de acesso para ECSs que têm os mesmos requisitos de proteção de segurança e são mutuamente confiáveis em uma VPC. Você pode criar um grupo de segurança e definir regras de acesso diferentes para proteger os ECSs que ele contém. Você pode criar e excluir grupos de segurança, adicionar, replicar, modificar, excluir, importar ou exportar regras de grupo de segurança, exibir o grupo de segurança de um ECS, alterar o grupo de segurança de um ECS e adicionar recursos de nuvem ou removê-los de um grupo de segurança. Para obter detalhes, consulte **Visão geral de grupo de segurança**.
	Network ACL	Uma network ACL é uma camada opcional de segurança para suas sub-redes. Você pode vincular uma ou mais sub-redes a uma network ACL para controlar o tráfego de entrada e saída das sub-redes. Você pode criar, exibir, modificar, excluir, habilitar, desabilitar network ACLs, associar sub-redes ou desassociá-las de network ACLs e adicionar, modificar, alterar a sequência de, habilitar, desabilitar e excluir regras de network ACL. Para obter detalhes, consulte **Visão geral de network ACL**.
EIP e largura de banda	EIP	Elastic IP (EIP) permite que você utilize endereços IP públicos estáticos e larguras de banda escaláveis para ligar os seus recursos da nuvem à Internet. Você pode atribuir EIPs, vincular EIPs a recursos de nuvem, desvincular EIPs de recursos de nuvem, liberar EIPs, modificar a largura de banda EIP e atualizar o BGP estático para o BGP dinâmico Para obter detalhes, consulte **Visão geral de EIP**.
	Largura de banda compartilhada	Largura de banda compartilhada permite que diversos EIPs compartilhem a mesma largura de banda. Todos os ECSs, BMSs e balanceadores de carga que tenham EIPs vinculados na mesma região podem compartilhar a mesma largura de banda. Você pode atribuir, modificar, excluir uma largura de banda compartilhada, adicionar EIPs a uma largura de banda compartilhada e remover EIPs de uma largura de banda compartilhada.

Categoria	Função	Descrição
Interconexão de recursos	Conexão de emparelhamento de VPC	A conexão de emparelhamento de VPC é uma conexão de rede entre duas VPCs. A conexão de emparelhamento de VPC permite que duas VPCs se comuniquem usando endereços IP privados como se estivessem na mesma VPC. Você pode criar uma conexão de emparelhamento de VPC entre suas próprias VPCs dentro da mesma região ou entre a sua VPC e a VPC de outra conta na mesma região. No entanto, não é possível criar uma conexão de emparelhamento de VPC entre VPCs em regiões diferentes. Você pode criar uma conexão de emparelhamento de VPC com outra VPC na sua conta ou com uma VPC em outra conta. Você também pode exibir, modificar e excluir conexões de emparelhamento de VPC. Para obter detalhes, consulte **Visão geral de emparelhamento de VPC**.
Monitoramento	Exibição de métricas	Você pode visualizar a largura de banda e o uso de EIP do serviço VPC por meio do Cloud Eye, criar e definir regras de alarme e personalizar os objetos monitorados e as políticas de notificação sem adicionar plug-ins. Para obter detalhes, consulte **Métricas suportadas**.
Auditoria	Exibição de registros de auditoria	Com o CTS, você pode gravar as operações executadas no serviço VPC para fins futuros de consulta, auditoria e rastreamento inverso. Você pode ver e exportar registros de operação dos últimos sete dias no console do CTS.
Tag	Gerenciamento de tags	As tags ajudam você a identificar e gerenciar os recursos da nuvem. Você pode gerenciar tags VPC, tags de sub-rede e tags de EIP.
Permissões	Gerenciamento de permissões	Você pode usar o Identity and Access Management (IAM) para implementar o gerenciamento de permissões refinado para suas VPCs, permitindo que as empresas definam permissões de acesso diferentes com base nas organizações e nas responsabilidades. Você pode criar um usuário do IAM, conceder permissões ao usuário e criar políticas de VPC personalizadas.

5 Segurança

5.1 Responsabilidades compartilhadas

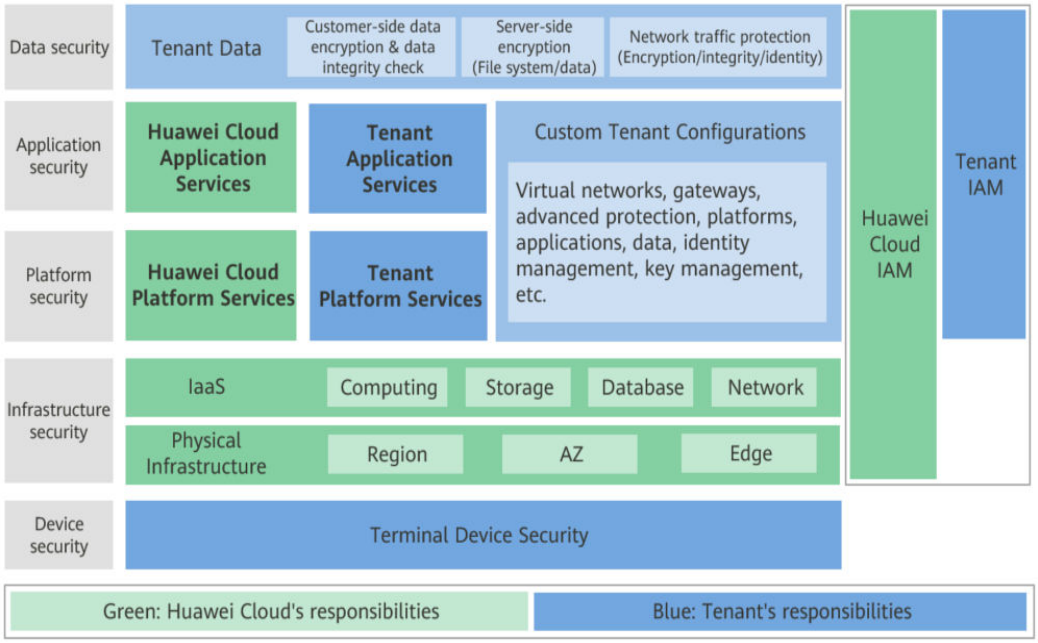
Huawei garante que seu compromisso com a segurança cibernética nunca será superado pela consideração de interesses comerciais. Para lidar com os desafios emergentes de segurança na nuvem e ameaças e ataques à segurança na nuvem, a Huawei Cloud constrói um sistema abrangente de garantia de segurança de 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 5-1 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 5-1 Modelo de responsabilidade de segurança compartilhada da Huawei Cloud



5.2 Identity Authentication and Access Control

Identity Authentication

Identity and Access Management (IAM) enables you to easily manage users and control their access to Huawei Cloud services and resources.

You can use IAM to control access to your VPC resources. IAM permissions define which actions on your cloud resources are allowed or denied.

After creating an IAM user, the administrator needs to add it to a user group and grant the permissions required by VPC to the user group. Then, all users in this group automatically inherit the granted permissions.

- **Permissões**

Access Control

- **Security Groups**

  A security group is a collection of access control rules for cloud resources, such as cloud servers, containers, and databases, that have the same security protection requirements and that are mutually trusted within a VPC. After a security group is created, you can create various access rules for the security group, these rules will apply to all cloud resources added to this security group.

  You can create and delete security groups, add, replicate, modify, delete, import or export security group rules, view or change the security group of an ECS, and add ECSs to or remove them from a security group.

  You can define access rules for a security group. Then these rules will apply to all cloud resources added to this security group.

- **Network ACLs**

A network ACL is an optional layer of security for your subnets. You can associate one or more subnets with a network ACL to control traffic in and out of the subnets.

You can create, view, modify, delete, enable, disable network ACLs, associate subnets with or disassociate them from network ACLs, add, modify, change the sequence of, enable, disable, and delete network ACL rules.

You can define network ACL rules to control traffic in and out of the subnets.

5.3 Auditing and Logging

Auditing

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.

After CTS is enabled, it can record VPC operations.

Logging

A VPC flow log records information about traffic going to and from your VPC. VPC flow logs help you monitor network traffic, analyze network attacks, and determine whether security group and network ACL rules require modification.

5.4 Monitoramento de riscos

Cloud Eye is a multi-dimensional resource monitoring platform. You can use Cloud Eye to monitor the utilization of service resources, track the running status of cloud services, configure alarm rules and notifications, and quickly respond to resource changes.

With Cloud Eye, you can view the bandwidth and EIP usage. You can also create alarm rules and configure monitoring thresholds and alarm notifications. This will ensure you learn about VPC resource status in a timely manner.

6 Observações e restrições

VPC

Tabela 6-1 lista as cotas de recursos da VPC por região para sua conta.

Tabela 6-1 Cotas de recursos da VPC

Recurso	Cota padrão	Ajustável
VPCs por conta	Como exibir minhas cotas?	Yes
Sub-redes por conta		Yes
Grupos de segurança por conta		Yes
Regras de grupo de segurança por conta		Yes
Rotas por tabela de rotas		Não
Tabela de rotas padrão por VPC		Yes
Conexões de emparelhamento de VPC por região		Não
Network ACLs por conta		Yes
ECSs que podem ser vinculados a um endereço IP virtual		Não
Logs de fluxo de VPC por conta		Não

NOTA

- A cota aplica-se a uma única conta
- Uma ACL da rede não pode conter mais de 20 regras em uma direção. Caso contrário, seu desempenho pode se deteriorar.

Grupo de segurança

- Por padrão, você pode criar um máximo de 100 grupos de segurança em sua conta de nuvem.
- Por padrão, não pode associar mais de cinco grupos de segurança a cada ECS ou NIC de extensão.
- Se um ECS ou uma NIC de extensão estiver associado a vários grupos de segurança, as regras de grupo de segurança serão aplicadas com base na seguinte sequência: o primeiro grupo de segurança associado terá precedência sobre os associados posteriormente e, em seguida, a regra com a prioridade mais alta nesse grupo de segurança será aplicada primeiro.
- Você pode adicionar no máximo 20 instâncias a um grupo de segurança por vez.
- Um grupo de segurança não pode ter mais do que instâncias de 6.000 associadas ou o desempenho se deteriorará.
- As regras de grupo de segurança com determinadas configurações não entram em vigor para ECSs de determinadas especificações. **Tabela 6-2** mostra os detalhes.

Tabela 6-2 Cenários em que as regras de grupo de segurança não entram em vigor

Configuração da regra	Tipo de ECS
Source ou **Destination** é definido como **IP address group**.	Os seguintes tipos de ECS x86 não são suportados: ● Computação geral (S1, C1 e C2 ECSs) ● Otimizado por memória (M1 ECSs) ● Computação de alto desempenho (H1 ECSs) ● Uso intensivo de disco (D1 ECSs) ● Acelerado por GPU (G1 e G2 ECSs) ● Ampla memória (E1, E2 e ET2 ECSs)
Port é definida como portas não consecutivas.	Os seguintes tipos de ECS x86 não são suportados: ● Computação geral (S1, C1 e C2 ECSs) ● Otimizado por memória (M1 ECSs) ● Computação de alto desempenho (H1 ECSs) ● Uso intensivo de disco (D1 ECSs) ● Acelerado por GPU (G1 e G2 ECSs) ● Ampla memória (E1, E2 e ET2 ECSs)
	Todos os flavors de ECS do Kunpeng não oferecem suporte a portas não consecutivas. Se você usar números de porta inconsecutivos em uma regra de grupo de segurança de um ECS de Kunpeng, essa regra e as regras configuradas após essa regra não terão efeito. Se configurar a regra de grupo de segurança A com portas inconsecutivas **22,24** e, em seguida, configurar a regra de grupo de segurança B com a porta 9096, a regra A e a regra B não terão efeito.

NOTA

- Para obter detalhes sobre ECSs x86, consulte **Especificações do ECS (x86)**.
- Para obter detalhes sobre os ECSs de Kunpeng, consulte **Especificações do ECS (Kunpeng)** .

ACL da rede

- By default, you can create a maximum of 200 ACLs da rede in your cloud account.
- A ACL da rede can contain no more than 20 rules in one direction, or performance will deteriorate.
- For optimal performance, import no more than 40 regra de ACLs da rede at a time. Existing rules will still be available after new rules are imported. Each rule can be imported only once.

Tabela de rotas

- Você pode adicionar rotas para, excluir rotas e modificar rotas na tabela de rotas padrão, mas não pode excluir a tabela.
- Ao criar uma conexão da VPN, Cloud Connect ou Direct Connect, a tabela de rotas padrão fornece automaticamente uma rota que não pode ser excluída ou modificada.

Conexão de emparelhamento de VPC

- Uma conexão de emparelhamento de VPC só pode conectar VPCs na mesma região.
  - Se você quiser conectar VPCs em regiões diferentes, use **Cloud Connect**.
  - Se você precisar de apenas alguns ECSs em regiões diferentes para se comunicar, poderá **atribuir e vincular EIPs aos ECSs**.
- Se as VPCs locais e de par tiverem blocos CIDR sobrepostos, a conexão de emparelhamento da VPC pode não ter efeito.

  Neste caso, você pode consultar **exemplos de configuração de rede**.
- Uma conexão de emparelhamento de VPC pode permitir que uma VPC criada no site da Huawei Cloud da China continental e outra criada no site da Huawei Cloud Internacional se comuniquem, mas as VPCs devem estar na mesma região. Por exemplo, uma VPC no site do China continental está na região CN-Hong Kong, e a outra VPC no site Internacional também está na região CN-Hong Kong.
- Por padrão, se a VPC A estiver emparelhada com a VPC B que tenha EIPs, a VPC A não poderá usar EIPs na VPC B para acessar a Internet. Para habilitar isso, você pode usar o serviço NAT Gateway ou configurar um servidor SNAT. Para obter detalhes, consulte **Habilitação da conectividade com a Internet para um ECS sem um EIP**.

Log de fluxo de VPC

- Atualmente, apenas ECSs S2, M2, Hc2, D2, Pi1, S3, C3, M3, H3, Ir3, I3, S6, E3, C3ne, M3ne, G5, P2v, C6, M6, Pi1 e H3 suportam logs de fluxo de VPC.

  Para obter detalhes sobre tipos de ECS, consulte **Tipos de ECS**.
- Por padrão, você pode criar no máximo 10 logs de fluxo de VPC.

Endereço IP virtual

- Os endereços IP virtuais não são recomendados quando várias NICs na mesma sub-rede são configuradas em um ECS. É muito fácil haver conflitos de rota no ECS, o que causaria falha de comunicação usando o endereço IP virtual.
- Um endereço IP virtual só pode ser vinculado a ECSs na mesma sub-rede.
- Recomenda-se que não mais de oito endereços IP virtuais sejam vinculados a um ECS.
- Recomenda-se que não mais de 10 ECSs sejam vinculados a um endereço IP virtual.

Largura de banda

- A menor largura de banda compartilhada que pode ser comprada é de 5 Mbit/s. Você só pode adicionar EIPs de pagamento por uso a uma largura de banda compartilhada.
- Cada conta pode ter um máximo de 5 larguras de banda compartilhadas. Se você precisar de mais larguras de banda compartilhadas, envie um tíquete de serviço para solicitar um aumento de cota.
- Dentro do período de validade de uma largura de banda usada por um EIP anual/mensal, você só pode aumentar o tamanho da largura de banda. Você só pode reduzir o tamanho da largura de banda ao renovar a assinatura.
- Se um EIP de pagamento por uso faturado pelo tráfego usar uma largura de banda dedicada, somente a largura de banda usada na direção de saída será cobrada.
- Uma largura de banda compartilhada ou largura de banda dedicada só pode ser usada por recursos pertencentes à mesma conta.

  NOTA

  - A largura de banda de entrada é a largura de banda consumida quando os dados são transferidos da Internet para a Huawei Cloud. A largura de banda de saída é a largura de banda consumida quando os dados são transferidos da Huawei Cloud para a Internet.
  - Em 31 de julho de 2020, 00:00:00 GMT + 08:00, as regras que limitam as larguras de banda públicas foram alteradas nas regiões da China continental, incluindo CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1 e CN North-Ulanqab1.

    Em 10 de dezembro de 2021, 00:00:00 GMT+08:00, as regras que limitam as larguras de banda públicas foram alteradas em CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, LA-Mexico City2, LA-Sao Paulo1 e LA-Santiago.

    Após a mudança:

    - Se a banda comprada ou modificada de até 10 Mbit/s, a largura de banda de entrada será de 10 Mbit/s, e a largura de banda de saída será a mesma que a largura de banda comprada ou modificada.
    - Se a largura de banda comprada ou modificada de mais de 10 Mbit/s, as larguras de banda nas direções de entrada e saída serão as mesmas que a largura de banda comprada ou modificada.

Pacotes de dados compartilhados

- Pacotes de dados compartilhados exigem um pagamento único e entram em vigor imediatamente após a compra. Não é possível especificar a data de efetivação.
- Pacotes de dados compartilhados não podem ser cancelados uma vez comprados e não podem ser renovados após a expiração.
- Pacotes de dados compartilhados são cobrados por mês ou ano. Uma vez expirada, a cota de pacote restante não pode mais ser usada.
- Pacotes de dados compartilhados só podem ser usados pela largura de banda de pagamento por uso cobrada pelo tráfego. Dois tipos de pacotes de dados compartilhados

estão disponíveis: BGP estático (para largura de banda de BGP estático) e BGP dinâmico (para largura de banda de BGP dinâmico).

- Um pacote de dados compartilhado não pode ser usado para a largura de banda de um EIP específico.
- Um pacote de dados compartilhado não pode ser usado para uma largura de banda compartilhada.
- Um pacote de dados compartilhado não pode ser usado por EIPs do tipo de BGP premium.
- Se você tem um pedido que não foi pago dentro do prazo de pagamento, você precisa cancelar ou pagar o pedido primeiro. Em seguida, você pode comprar um pacote de dados compartilhado.

7 VPC e outros serviços

Figura 7-1 mostra a relação entre a VPC e outros serviços.

Figura 7-1 VPC e outros serviços

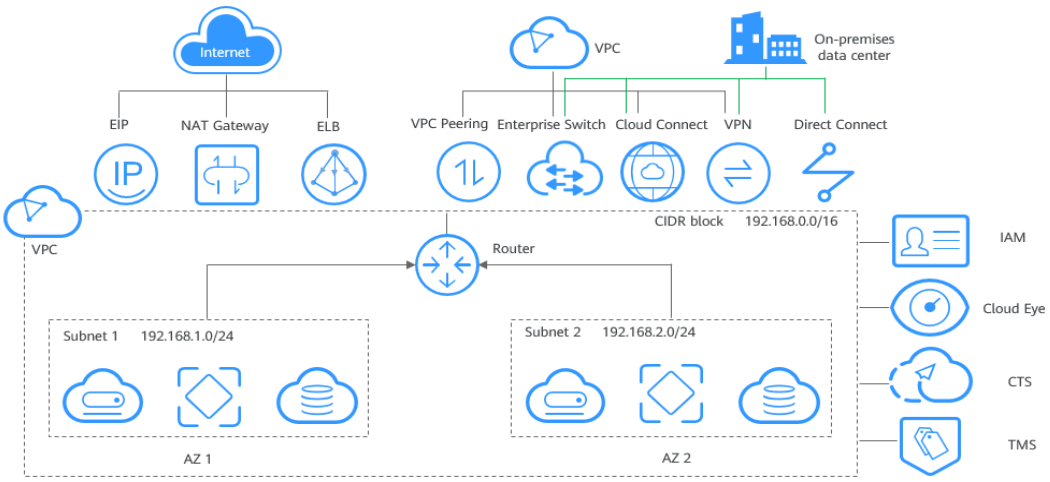


Tabela 7-1 Serviços relacionados

Função interativa	Serviço	Referência
Redes seguras para ECSs.	Elastic Cloud Server (ECS)	**Adição uma regra de grupo de segurança**
Conetar ECSs em uma VPC à Internet.	Elastic IP (EIP)	**Conexão de ECSs em uma VPC à Internet usando EIPs**
	NAT Gateway	**Uso da SNAT para acessar a Internet**
Conetar uma VPC a um data center local.	Virtual Private Network (VPN)	**Virtual Private Network**
	Direct Connect	**Direct Connect**

Função interativa	Serviço	Referência
Distribuir o tráfego de entrada para vários ECSs em uma VPC.	Elastic Load Balance (ELB)	**Elastic Load Balance**
Atribuir permissões diferentes aos funcionários da sua empresa para acessar seus recursos de VPC.	Identity and Access Management (IAM)	**Identity and Access Management**
Verificar a largura de banda e o uso do tráfego.	Cloud Eye	**Visualização de métricas**
Registra operações relacionadas à VPC para posterior consulta, auditoria e retrocesso.	Cloud Trace Service (CTS)	**Exibição de logs de auditoria**
As tags identificam os recursos da VPC para facilitar a categorização e a pesquisa rápida.	Tag Management Service (TMS)	**Gerenciamento de tags do EIP**

8 Cobrança

Itens cobrados

O serviço de VPC é gratuito.

Tabela 8-1 Itens cobrados

Item cobrado	Descrição
EIP	EIPs são necessários se seus recursos precisarem acessar a Internet.

O serviço de EIP fornece vários modos de cobrança.

- **Modos de cobrança do EIP**
- **Qual opção de cobrança é certa para mim?**
- **Como serei cobrado se eu mudar meu tamanho de largura de banda?**
- **Como alterar o modo de cobrança de EIP?**

Modos de cobrança do EIP

Os EIPs podem ser cobrados em uma base anual/mensal ou de pagamento por uso. As opções de cobrança e os itens de cobrança dependem do modo de cobrança.

- **Figura 8-1**
- **Tabela 8-2**

Figura 8-1 Cobrança de EIP

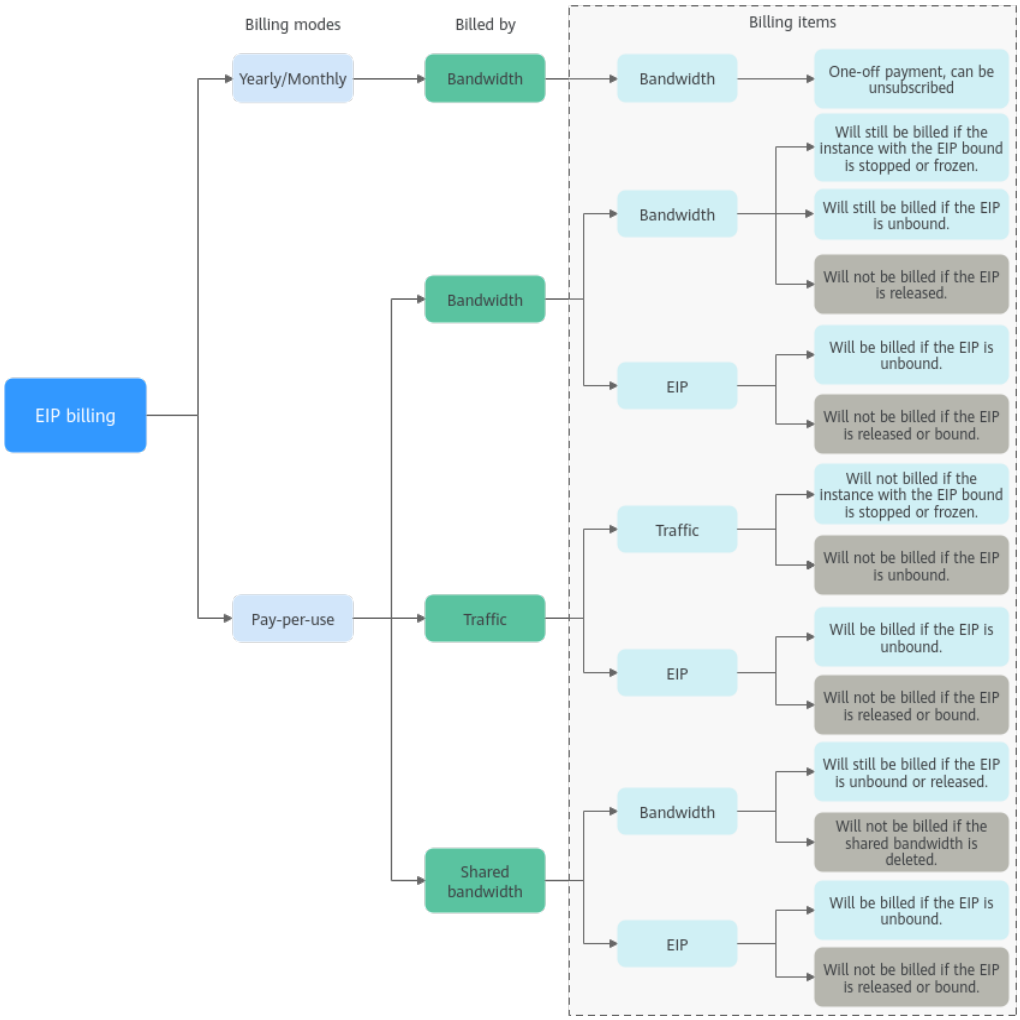


Tabela 8-2 Descrição da cobrança de EIP

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança	Impacto das operações de EIP nos itens de cobrança
Anual/Mensal	Largura de banda	Largura de banda	Se você comprar um EIP anual/mensal, precisará pagar apenas pela largura de banda incluída na assinatura. Você é cobrado com base no tamanho da largura de banda e na duração de uso especificados. Não há limite de quanto tráfego você pode usar.	Você pode cancelar a assinatura de uma assinatura anual/mensal. Sua taxa de uso real e algumas taxas preferenciais serão deduzidas do valor do reembolso.

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança	Impacto das operações de EIP nos itens de cobrança
Pagamento por uso	Largura de banda	• Largura de banda • EIP	Se um EIP de pagamento por uso for cobrado por largura de banda: • Largura de banda: você é cobrado com base no tamanho da largura de banda e na duração de uso especificados. Não há limite de quanto tráfego você pode usar. Depois que o EIP for comprado, você poderá alterar o tamanho da largura de banda especificada. A largura de banda que você usa não excederá a largura de banda especificada. • Retenção de EIP: se um EIP não for liberado, ele continuará sendo cobrado mesmo que não esteja vinculado a uma instância.	Após a compra de um EIP: • Se o EIP não estiver vinculado a nenhuma instância, tanto o EIP quanto sua largura de banda serão cobrados. • Se o EIP estiver vinculado a uma instância, somente a largura de banda será faturada. **A largura de banda será cobrada independentemente de a instância vinculada ao EIP estar em execução ou não.** • **Depois que o EIP for desvinculado de uma instância, a largura de banda continuará a ser cobrada. A menos que seja liberado, o EIP ainda será cobrado.** • Se o EIP for liberado, tanto o EIP quanto sua largura de banda não serão cobrados.

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança	Impacto das operações de EIP nos itens de cobrança
	Tráfego	● Tráfego ● EIP	Se um EIP de pagamento por uso for cobrado por tráfego: ● Tráfego: você é cobrado com base no seu tipo de EIP e na quantidade total de tráfego saindo da nuvem. O tamanho da largura de banda que você define é usado apenas para limitar a taxa máxima de transferência de dados. Para evitar altas taxas causadas pelo tráfego de intermitência, especifique um tamanho de largura de banda adequado ao comprar um EIP. ● Retenção de EIP: se um EIP não for liberado, ele continuará sendo cobrado mesmo que não esteja vinculado a uma instância.	Após a compra de um EIP: ● Se o EIP não estiver vinculado a uma instância, você será cobrado pelo próprio EIP, mas não pelo tráfego. ● Se o EIP estiver vinculado a uma instância, somente o tráfego usado será cobrado. **Se a instância vinculada ao EIP parar de ser executada e não houver tráfego gerado, não haverá taxas de tráfego nem de EIP.** ● **Depois que o EIP for desvinculado de uma instância, o tráfego não será cobrado, mas o EIP ainda será cobrado.** ● Se o EIP for liberado, o EIP não será cobrado.

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança	Impacto das operações de EIP nos itens de cobrança
	Largura de banda compartilhada	• Largura de banda compartilhada • EIP	Se um EIP de pagamento por uso for adicionado a uma largura de banda compartilhada: • Largura de banda compartilhada: somente a largura de banda compartilhada será cobrada. Não haverá custos adicionais de largura de banda ou tráfego para EIPs adicionados à largura de banda compartilhada. • Retenção de EIP: se um EIP não for liberado, ele continuará sendo cobrado mesmo que não esteja vinculado a uma instância.	Após a compra de um EIP: • Largura de banda compartilhada – Nenhuma operação no EIP afetará a cobrança de uma largura de banda compartilhada. Por exemplo, se você liberou o EIP, mas não excluiu a largura de banda compartilhada, a largura de banda compartilhada ainda será cobrada. – Depois que uma largura de banda compartilhada for excluída, ela não será mais cobrada. • EIP – Se o EIP não estiver vinculado a uma instância, o EIP ainda será cobrado. – Se o EIP for desvinculado de uma instância, ele será cobrado para mantê-lo alocado à sua conta, a menos que seja liberado. – Se o EIP for liberado ou vinculado a uma instância, o EIP não será cobrado.

Para economizar dinheiro, você pode adicionar vários EIPs na mesma região a uma largura de banda compartilhada. Uma largura de banda compartilhada pode ser cobrada em uma base

anual/mensal ou de pagamento por uso. Para obter detalhes, consulte **Tabela 8-3**. Atualmente, apenas EIPs de pagamento por uso podem ser adicionados a uma largura de banda compartilhada.

- Você pode adicionar um EIP a uma largura de banda compartilhada ao comprar o EIP.
- Você também pode adicionar um EIP existente a uma largura de banda compartilhada. Depois que o EIP é adicionado a uma largura de banda compartilhada, não haverá largura de banda adicional ou custo de tráfego. Você será cobrado apenas pela largura de banda compartilhada.

Tabela 8-3 Detalhes de cobrança de largura de banda compartilhada

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança
Anual/ Mensal	Largura de banda	Largura de banda	Se você comprar uma largura de banda compartilhada anual/mensal, será cobrado com base no tamanho da largura de banda especificada e na duração de uso. Não há limite de quanto tráfego você pode usar.
Pagamento por uso	Largura de banda	Largura de banda	você é cobrado com base no tamanho da largura de banda e na duração de uso especificados. Não há limite de quanto tráfego você pode usar. Depois que uma largura de banda compartilhada é comprada, você pode alterar o tamanho da largura de banda especificada. A largura de banda que você usa não excederá a largura de banda especificada.

NOTA

- O preço da largura de banda, tráfego e EIP depende da região.
- A largura de banda de EIP é a largura de banda de saída consumida quando os dados são transferidos da Huawei Cloud para a Internet. Por exemplo, quando os ECSs fornecem serviços acessíveis da Internet e usuários externos baixam recursos dos ECSs, isso consome a largura de banda de saída. Somente a largura de banda de saída será cobrada.
  - Se a largura de banda comprada ou modificada não for superior a 10 Mbit/s, a largura de banda de entrada será de 10 Mbit/s e a largura de banda de saída será a mesma que a largura de banda comprada ou modificada.
  - Se a largura de banda comprada ou modificada for superior a 10 Mbit/s, ambas as larguras de banda nas direções de entrada e saída serão iguais à largura de banda comprada ou modificada.

Qual opção de cobrança é certa para mim?

Os EIPs podem ser cobrados por largura de banda ou tráfego. **Tabela 8-4** mostra os cenários de aplicações de diferentes opções de cobrança.

O Cloud Eye monitora suas métricas de rede, como largura de banda e tráfego. Com base no uso da largura de banda, você pode determinar qual opção de cobrança (por largura de banda ou por tráfego) é mais econômica. Aqui estão algumas sugestões para sua referência:

- Se você precisar de menos de 5 Mbit/s de largura de banda por um curto período de tempo e o tráfego for leve, defina seu EIP para ser cobrado por tráfego.
- Se você precisa de menos de 5 Mbit/s de largura de banda, mas o tráfego é pesado, defina seu EIP para ser cobrado por largura de banda e escolha a cobrança anual/mensal ou de pagamento por uso, dependendo de quanto tempo você precisará da largura de banda.
- Se você precisar de mais de 5 Mbit/s de largura de banda e o uso da largura de banda for maior que 20%, defina seu EIP para ser cobrado por largura de banda.

Para obter detalhes, consulte **Visualização de métricas**.

Tabela 8-4 Cenários de aplicações de opções de cobrança de EIP

Modo de cobrança	Cobrado por	Cenário
Anual/ Mensal	Largura de banda	Tráfego pesado ou estável
Pagamento por uso	Largura de banda	Tráfego pesado ou estável
	Tráfego	Tráfego leve ou muito flutuante
	Largura de banda compartilhada	Tráfego escalonado

Como serei cobrado se eu mudar meu tamanho de largura de banda?

Se um EIP não for adicionado a uma largura de banda compartilhada, o EIP usará a largura de banda dedicada, independentemente de ela ser cobrada por largura de banda ou tráfego. Depois que um EIP é adicionado a uma largura de banda compartilhada, somente a largura de banda compartilhada é cobrada.

- **Modificação do tamanho da largura de banda dedicada**
- **Modificação do tamanho da largura de banda compartilhada**

Quando você altera o tamanho da largura de banda, o preço da largura de banda e o tempo efetivo dependem do modo de cobrança, que se aplica a larguras de banda dedicadas e compartilhadas. Para obter detalhes, consulte **Tabela 8-5**.

NOTA

A diminuição das larguras de banda pode causar perda de pacotes.

Tabela 8-5 Impacto na cobrança após a alteração do tamanho da largura de banda

Modo de cobrança	Cobrado por	Alteração	Impacto
Anual/ Mensal	Largura de banda	Aumentar a largura de banda	A alteração entrará em vigor imediatamente. O aumento da largura de banda será cobrado de acordo.
	Largura de banda	Diminuir a largura de banda após a renovação	A alteração não entrará em vigor imediatamente. Você precisa selecionar um novo tamanho de largura de banda e uma duração de renovação. A alteração entrará em vigor no primeiro ciclo de cobrança após uma renovação bem-sucedida. ● O pedido pode ser cancelado antes que a largura de banda entre em vigor. ● A largura de banda não pode ser modificada no primeiro ciclo de cobrança.
Pagamento por uso	Largura de banda	Aumentar ou diminuir a largura de banda	A alteração entrará em vigor imediatamente.
	Tráfego	Aumentar ou diminuir a largura de banda	A alteração entrará em vigor imediatamente. O tamanho da largura de banda que você define é usado apenas para limitar a taxa máxima de transferência de dados.

Como alterar o modo de cobrança de EIP?

O serviço EIP tem vários modos de cobrança que você pode escolher. Você pode alterar o modo de cobrança do EIP durante o período de uso do EIP, se necessário.

- **Tabela 8-6**
- **Alteração da cobrança da largura de banda**

NOTA

Alterar o modo de cobrança não altera os EIPs nem interrompe seu uso.

Figura 8-2 Alteração do modo de cobrança do EIP

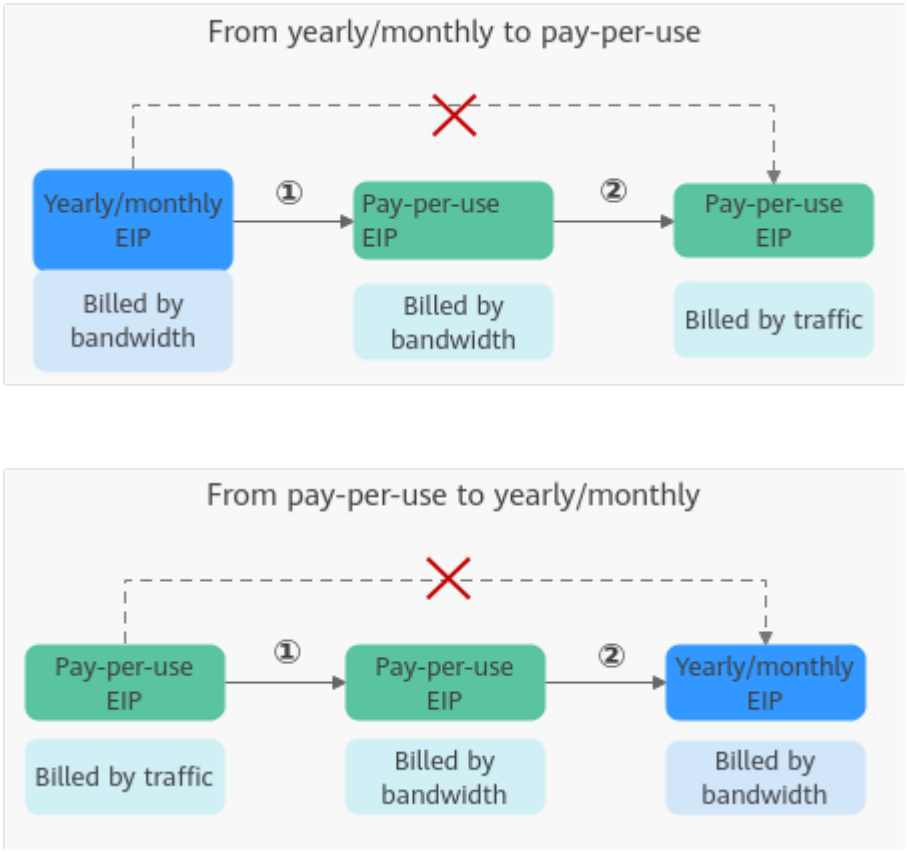


Tabela 8-6 Descrição da alteração do modo de cobrança de EIP

Alteração	Descrição
De anual/mensal para pagamento por uso	● Um EIP cobrado em uma base anual/mensal pode ser alterado diretamente para ser cobrado por largura de banda em uma base de pagamento por uso após a expiração. ● Um EIP cobrado em uma base anual/mensal não pode ser alterado diretamente para ser cobrado pelo tráfego em uma base de pagamento por uso. Para alterar isso: 1. Altere o EIP para ser cobrado por largura de banda em uma base de pagamento por uso. 2. Altere o EIP para ser cobrado por tráfego em uma base de pagamento por uso. O novo modo de cobrança entra em vigor somente após a expiração da assinatura anual/mensal.

Alteração	Descrição
De pagamento por uso a anual/ mensal	● Um EIP que é cobrado por largura de banda em uma base de pagamento por uso pode ser alterado diretamente para ser cobrado em uma base anual/ mensal. ● Um EIP que é cobrado por tráfego em uma base de pagamento por uso não pode ser alterado diretamente para ser cobrado em uma base anual/ mensal. Para alterar isso: 1. Altere o EIP para ser cobrado por largura de banda em uma base de pagamento por uso. 2. Altere o EIP a ser cobrado anualmente/ mensalmente. O novo modo de cobrança entra em vigor imediatamente.
● Da cobrança por tráfego (pagamento por uso) à cobrança por largura de banda (pagamento por uso) ● Da cobrança por largura de banda (pagamento por uso) à cobrança por tráfego (pagamento por uso)	● Um EIP cobrado por tráfego em uma base de pagamento por uso pode ser alterado diretamente para ser cobrado por largura de banda em uma base de pagamento por uso. ● Um EIP cobrado por largura de banda em uma base de pagamento por uso pode ser alterado diretamente para ser cobrado pelo tráfego em uma base de pagamento por uso. O novo modo de cobrança entra em vigor imediatamente.

9 Permissões

Se você precisar atribuir permissões diferentes aos funcionários da sua empresa para acessar suas VPCs, 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 acessar aos seus recursos da Huawei Cloud com segurança.

Com o IAM, você pode criar usuários do IAM e atribuir permissões para controlar seu acesso aos recursos específicos. Por exemplo, se você quiser que alguns desenvolvedores de software em sua empresa usem VPCs, mas não quiser que eles excluam VPCs ou executem outras operações de alto risco, poderá conceder permissões para usar VPCs, mas não permissões para excluí-las.

Se a sua HUAWEI ID não necessitar do IAM para gestão de permissões, pode ignorar esta secção.

O IAM é um serviço gratuito. Você paga apenas pelos recursos na sua conta. Para obter mais informações, consulte **Visão geral de serviço IAM**.

Permissões de VPC

Novos usuários do IAM não têm permissões atribuídas por padrão. Você precisa em primeiro adicionar um usuário 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.

VPC é um serviço no nível do projeto implementado para regiões específicas. Quando você define **Scope** como **Region-specific projects** e seleciona os projetos especificados (por exemplo, **ap-southeast-1**) nas regiões especificadas (por exemplo, **CN-Hong Kong**), os usuários só têm permissões para VPCs nos projetos selecionados. Se você definir **Scope** como **All resources**, os usuários terão permissões para VPCs em todos os projetos específicos da região. Ao acessar VPCs, os usuários precisam mudar para a região autorizada.

Você pode conceder permissões usando funções e políticas.

- Funções: uma estratégia de autorização grosseira 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. Ao conceder permissões usando funções, você também precisa anexar funções dependentes. 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 da nuvem sob determinadas condições.

Esse tipo de autorização é mais flexível e é ideal para acesso de privilégio mínimo. Por exemplo, você pode conceder aos usuários da VPC somente as permissões para gerenciar um determinado tipo de recursos. 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 pela VPC, consulte **Políticas de permissões e ações suportadas**.

Tabela 9-1 lista todas as permissões definidas pelo sistema para a VPC.

Tabela 9-1 Permissões definidas pelo sistema para VPC

Nome da política	Descrição	Tipo de política	Dependências
VPC FullAccess	Permissões completas para VPC	Política definida pelo sistema	Para usar a função de log de fluxo da VPC, os usuários também devem ter a permissão **LTS ReadOnlyAccess**.
VPC ReadOnlyAccess	Permissões somente leitura na VPC.	Política definida pelo sistema	Nenhuma
VPC Administrator	A maioria das permissões na VPC, excluindo a criação, modificação, exclusão e exibição de grupos de segurança e regras de grupo de segurança. Para receber essa permissão, os usuários também devem ter a permissão **Tenant Guest**.	Função definida pelo sistema	Política **Tenant Guest**, que deve ser anexada ao mesmo projeto que **VPC Administrator**.

Tabela 9-2 lista as operações comuns compatíveis com as permissões definidas pelo sistema para VPC.

Tabela 9-2 Operações comuns compatíveis com as permissões definidas pelo sistema

Operação	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Criar uma VPC	x	√	√
Modificar uma VPC	x	√	√
Excluir uma VPC	x	√	√

Operação	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Exibir informações da VPC	√	√	√
Criar uma sub-rede	x	√	√
Exibir informações de sub-rede	√	√	√
Modificar uma sub-rede	x	√	√
Excluir uma sub-rede	x	√	√
Criar um grupo de segurança	x	x	√
Exibir informações do grupo de segurança	√	x	√
Modificar um grupo de segurança	x	x	√
Excluir um grupo de segurança	x	x	√
Adicionar uma regra de grupo de segurança	x	x	√
Exibir uma regra de grupo de segurança	√	x	√
Modificar uma regra de grupo de segurança	x	x	√
Excluir uma regra de grupo de segurança	x	x	√
Criar uma ACLs da rede	x	√	√
Visualizar uma ACLs da rede	√	√	√

Operação	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Modificar uma ACLs da rede	x	√	√
Excluir uma ACLs da rede	x	√	√
Adicionar uma regra de ACLs da rede	x	√	√
Modificar uma regra de ACLs da rede	x	√	√
Excluir uma regra de ACLs da rede	x	√	√
Criar uma conexão de emparelhamento de VPC	x	√	√
Modificar uma conexão de emparelhamento de VPC	x	√	√
Excluir uma conexão de emparelhamento de VPC	x	√	√
Consultar uma conexão de emparelhamento de VPC	√	√	√
Aceitar uma solicitação de conexão de emparelhamento de VPC	x	√	√
Recusar uma solicitação de conexão de emparelhamento de VPC	x	√	√
Criar uma tabela de rotas	x	√	√

Operação	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Excluir uma tabela de rotas	x	√	√
Modificar uma tabela de rotas	x	√	√
Associar uma tabela de rotas a uma sub-rede	x	√	√
Adicionar uma rota	x	√	√
Modificar uma rota	x	√	√
Excluir uma rota	x	√	√
Criar um log de fluxo de VPC	x	√	√
Exibir um log de fluxo de VPC	√	√	√
Ativar ou desativar um log de fluxo de VPC	x	√	√
Excluir um log de fluxo de VPC	x	√	√

Links úteis

- **O que é o IAM?**
- **Criação de um usuário e concessão de permissões da VPC**
- **Políticas de permissões e ações suportadas**

10 Conceitos básicos

10.1 Sub-rede

Uma sub-rede é um bloco CIDR único com um intervalo de endereços IP em uma VPC. Todos os recursos em uma VPC devem ser implementados em sub-redes.

- Por padrão, os ECSs em todas as sub-redes da mesma VPC podem se comunicar uns com os outros, mas os ECSs em diferentes VPCs não.

  Você pode criar conexões de emparelhamento de VPC para permitir que ECSs em VPCs diferentes, mas na mesma região, se comuniquem entre si. Para obter detalhes, consulte **Visão geral da conexão de emparelhamento de VPC**.

- Depois que uma sub-rede é criada, seu bloco CIDR não pode ser modificado.

  Ao criar uma VPC, uma sub-rede padrão será criada em conjunto. Se você precisar de mais sub-redes, consulte **Criação de uma sub-rede para a VPC**.

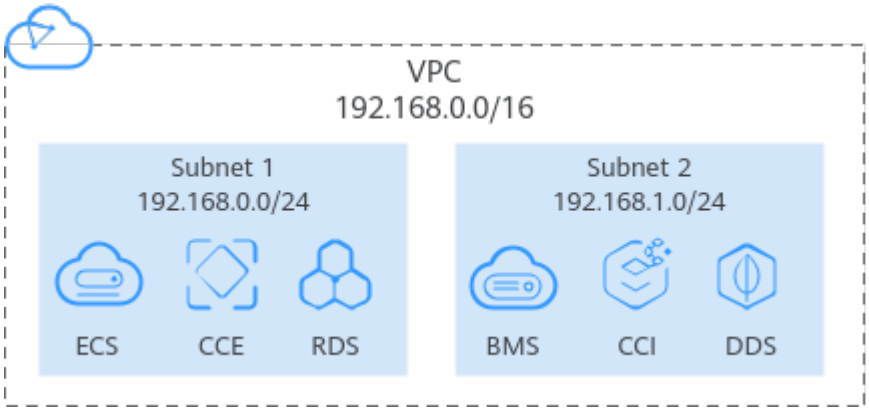
  As sub-redes usadas para implantar seus recursos devem residir na VPC, e as máscaras de sub-rede usadas para defini-las podem estar entre a máscara de rede do bloco CIDR da VPC e a máscara de rede /28.

  – 10.0.0.0 – 10.255.255.255
  – 172.16.0.0 – 172.31.255.255
  – 192.168.0.0 – 192.168.255.255

  NOTA

  Uma máscara de sub-rede pode estar entre a máscara de rede do bloco CIDR da VPC e a máscara de rede /28. Se um bloco CIDR da VPC for 192.168.0.0/16, sua máscara de sub-rede poderá ter entre 16 e 28.

Figura 10-1 Sub-rede

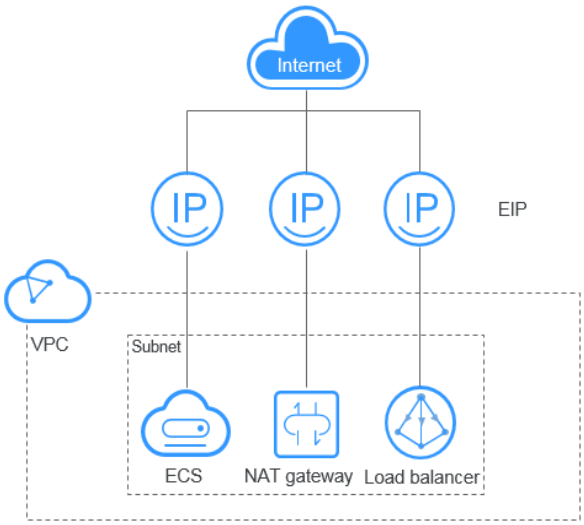


10.2 Elastic IP

O serviço Elastic IP (EIP) permite que seus recursos de nuvem se comuniquem com a Internet usando endereços IP públicos estáticos e larguras de banda escaláveis. Os EIP podem ser vinculados ou não dos ECSs, BMS, endereços IP virtuais, gateways NAT, ou balanceadores de carga.

Cada EIP pode ser usado por apenas um recurso de nuvem por vez.

Figura 10-2 Acessar a Internet usando um EIP



10.3 Tabela de rotas

Tabelas de rotas

Uma tabela de rotas contém um conjunto de rotas que são usadas para determinar para onde o tráfego de rede das suas sub-redes em uma VPC é direcionado. Cada sub-rede deve estar associada a uma tabela de rotas. Você pode associar uma sub-rede a apenas uma tabela de rotas por vez, mas pode associar várias sub-redes à mesma tabela de rotas.

As rotas IPv4 e IPv6 são suportadas.

Figura 10-3 Tabela de rotas

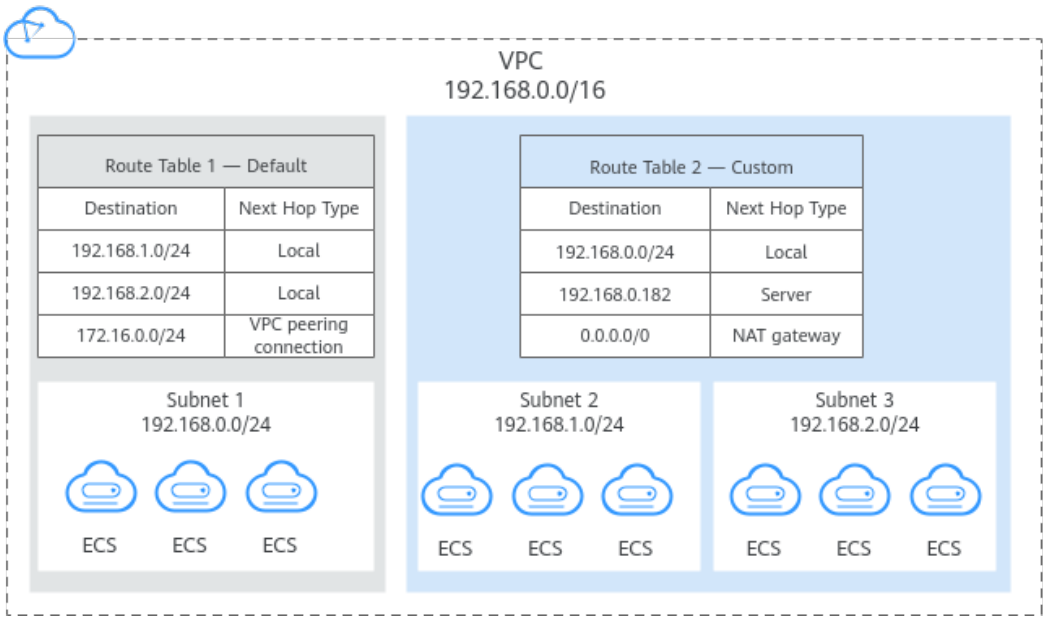


Tabela de rota padrão e tabela de rota personalizada

Quando uma VPC é criada, o sistema gera automaticamente uma tabela de rotas padrão para ela. Se você criar uma sub-rede na VPC, a sub-rede será associada automaticamente à tabela de rotas padrão.

- Você pode adicionar rotas para, excluir rotas e modificar rotas na tabela de rotas padrão, mas não pode excluir a tabela.
- Ao criar uma conexão da VPN, Cloud Connect ou Direct Connect, a tabela de rotas padrão fornece automaticamente uma rota que não pode ser excluída ou modificada.

Se você não quiser usar a tabela de rotas padrão, você pode criar uma tabela de rotas personalizada e vincular com a sub-rede. Você pode excluir a tabela de rota personalizada se não for mais necessária.

NOTA

- A tabela de rota personalizada associada a uma sub-rede afeta apenas o tráfego de saída. A tabela de rotas padrão determina o tráfego de entrada.
- Para usar uma tabela de rotas personalizada, você precisa enviar um tíquete de serviço. Você precisa clicar em **Increase quota** na página **Create Route Table** ou escolher **More** > **Service Tickets** > **Create Service Ticket** no canto superior direito da página. Para obter mais informações, consulte **Envio de um tíquete de serviço**.

Rota

Uma rota é configurada com o destino, o tipo de próximo salto e o próximo salto para determinar para onde o tráfego de rede é direcionado. As rotas são classificadas em rotas do sistema e rotas personalizadas.

- Rotas do sistema: essas rotas são adicionadas automaticamente pelo sistema e não podem ser modificadas ou excluídas.

Depois que uma tabela de rotas é criada, o sistema adiciona automaticamente as seguintes rotas do sistema à tabela de rotas, para que as instâncias em uma VPC possam se comunicar entre si.

– Rotas cujo destino é 100.64.0.0/10 ou 198.19.128.0/20.
– Rotas cujo destino é um bloco CIDR de sub-rede.

  Se você ativar o IPv6 ao criar uma sub-rede, o sistema atribuirá automaticamente um bloco CIDR IPv6 à sub-rede. Em seguida, você pode exibir rotas IPv6 em sua tabela de rotas. Exemplos de destinos de blocos CIDR de sub-rede são os seguintes:

  - IPv4: 192.168.2.0/24
  - IPv6: 2407:c080:802:be7::/64

  NOTA

  Além das rotas do sistema anteriores, o sistema adiciona automaticamente uma rota cujo destino é 127.0.0.0/8. Este é o endereço de loopback local.

- Rotas personalizadas: estas são rotas que você pode adicionar, modificar e excluir. O destino de uma rota personalizada não pode se sobrepor ao de uma rota do sistema.

  Você pode adicionar uma rota personalizada e configurar o destino, o tipo de próximo salto e o próximo salto na rota para determinar para onde o tráfego de rede será direcionado. **Tabela 10-1** lista os tipos suportados de próximos saltos.

  Não é possível adicionar duas rotas com o mesmo destino a uma tabela de rotas da VPC, mesmo que seus próximos tipos de salto sejam diferentes. A prioridade da rota depende do destino. De acordo com a regra de roteamento de correspondência mais longa, o destino com um grau de correspondência mais alto é preferencialmente selecionado para encaminhamento de pacotes.

Tabela 10-1 Tipo de próximo salto

Tipo de próximo salto	Descrição	Tabela de rotas suportadas
Servidor	O tráfego destinado ao destino é encaminhado para um ECS na VPC.	● Tabela de rota padrão ● Tabela de rota personalizada
NIC de extensão	O tráfego destinado ao destino é encaminhado para a NIC de extensão de um ECS na VPC.	● Tabela de rota padrão ● Tabela de rota personalizada
Rede definida pelo usuário do BMS	O tráfego endereçado ao destino é encaminhado para uma rede definida pelo usuário do BMS.	● Tabela de rota padrão ● Tabela de rota personalizada
Gateway de VPN	O tráfego destinado ao destino é encaminhado para um gateway de VPN.	Tabela de rota personalizada

Tipo de próximo salto	Descrição	Tabela de rotas suportadas
Gateway da Direct Connect	O tráfego destinado ao destino é encaminhado para um gateway da Direct Connect.	Tabela de rota personalizada
Conexão em nuvem	O tráfego endereçado ao destino é encaminhado para uma conexão em nuvem	Tabela de rota personalizada
Interface de rede suplementar	O tráfego endereçado ao destino é encaminhado à interface de rede suplementar de um ECS na VPC.	● Tabela de rota padrão ● Tabela de rota personalizada
Gateway de NAT	O tráfego destinado ao destino é encaminhado para um gateway de NAT.	● Tabela de rota padrão ● Tabela de rota personalizada
Conexão de emparelhamento de VPC	O tráfego destinado ao destino é encaminhado para uma conexão de emparelhamento de VPC.	● Tabela de rota padrão ● Tabela de rota personalizada
Endereço IP virtual	O tráfego destinado ao destino é encaminhado para um endereço IP virtual e, em seguida, enviado para ECSs ativos e em espera aos quais o endereço IP virtual está vinculado.	● Tabela de rota padrão ● Tabela de rota personalizada
Ponto de extremidade da VPC	O tráfego destinado ao destino é encaminhado para um ponto de extremidade da VPC.	● Tabela de rota padrão ● Tabela de rota personalizada
Contêiner em nuvem	O tráfego endereçado ao destino é encaminhado para um contêiner em nuvem.	● Tabela de rota padrão ● Tabela de rota personalizada
Roteador empresarial	O tráfego endereçado ao destino é encaminhado para um roteador empresarial.	● Tabela de rota padrão ● Tabela de rota personalizada
Firewall em nuvem	O tráfego endereçado ao destino é encaminhado para um firewall em nuvem.	● Tabela de rota padrão ● Tabela de rota personalizada

NOTA

Se você especificar o destino ao criar um recurso, uma rota do sistema será entregue. Se você não especificar um destino ao criar um recurso, uma rota personalizada que pode ser modificada ou excluída será entregue.

Por exemplo, quando você cria um gateway da NAT, o sistema entrega automaticamente uma rota personalizada sem um destino específico (0.0.0.0/0 é usado por padrão). Nesse caso, você pode alterar o destino. No entanto, quando você cria um gateway de VPN, você precisa especificar a sub-rede remota, ou seja, o destino de uma rota. Nesse caso, o sistema entrega essa rota do sistema. Não modifique o destino da rota na página **Route Tables**. Se o fizer, o destino será inconsistente com a sub-rede remota configurada. Para modificar o destino da rota, vá para a página de recursos específica e modifique a sub-rede remota. Em seguida, o destino da rota será alterado de acordo.

10.4 Grupo de segurança

Um grupo de segurança é uma coleção de regras de controle de acesso para recursos de nuvem, como servidores de nuvem, contêineres e bancos de dados, que têm os mesmos requisitos de proteção de segurança e que são mutuamente confiáveis. Depois que um grupo de segurança é criado, você pode criar várias regras de acesso para o grupo de segurança, essas regras serão aplicadas a todos os recursos em nuvem adicionados a esse grupo de segurança.

Assim como as listas brancas, as regras de grupo de segurança funcionam da seguinte maneira:

- As regras de entrada controlam o tráfego de entrada para instâncias no grupo de segurança. Se uma solicitação de entrada corresponder à origem em uma regra de grupo de segurança de entrada com **Action** definida como **Allow**, a solicitação será permitida.

  A menos que especificado de outra forma, você não precisa configurar regras de negação na direção de entrada porque as solicitações que não correspondem a regras de permissão serão negadas.
- As regras de saída controlam o tráfego de saída das instâncias da nuvem no grupo de segurança. Se o destino de uma regra de grupo de segurança de saída com **Action** definida como **Allow** for 0.0.0.0/0, todas as solicitações de saída serão permitidas.

  0.0.0.0/0 representa todos os endereços IPv4.

  ::/0 representa todos os endereços IPv6.

Tabela 10-2 mostra as regras de entrada e saída no grupo de segurança sg-AB.

Tabela 10-2 Regras no grupo de segurança sg-AB

Direção	Ação	Tipo	Protocolo & porta	Origem/ Destino	Descrição
Entrada	Allow	IPv4	Todos	Origem: sg-AB	Essa regra permite que os ECSs do grupo de segurança se comuniquem entre si.

Direção	Ação	Tipo	Protocolo & porta	Origem/ Destino	Descrição
Entrada	Allow	IPv4	TCP: 22	Origem: 0.0.0.0/0	Essa regra permite que todos os endereços IPv4 acessem ECSs no grupo de segurança pela porta SSH 22 para efetuar logon remotamente em ECSs de Linux.
Entrada	Allow	IPv4	TCP: 3389	Origem: 0.0.0.0/0	Essa regra permite que todos os endereços IPv4 acessem ECSs no grupo de segurança pela porta RDP 3389 para efetuar logon remotamente em ECSs do Windows.
Entrada	Allow	IPv4	TCP: 80	Origem: 10.5.6.30/32	Essa regra permite que o endereço IP 10.5.6.30 acesse ECSs no grupo de segurança pela porta 80.
Saída	Allow	IPv4	Todos	Destino: 0.0.0.0/0	Essa regra permite o acesso de ECSs no grupo de segurança a qualquer endereço IPv4 em qualquer porta.
Saída	Allow	IPv6	Todos	Destino: ::/0	Essa regra permite o acesso de ECSs no grupo de segurança a qualquer endereço IPv6 em qualquer porta.
Saída	Allow	IPv4	TCP: 80	Destino: 10.7.6.51/32	Essa regra permite o acesso de ECSs no grupo de segurança ao endereço IP 10.7.6.51 pela porta 80.

10.5 Conexão de emparelhamento de VPC

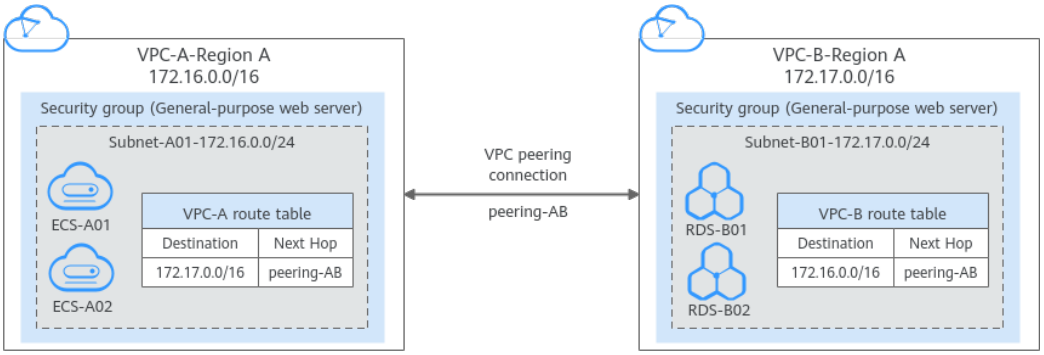
Uma conexão de emparelhamento de VPC é uma conexão de rede entre duas VPCs e permite que elas se comuniquem usando endereços IP privados. As VPCs a serem emparelhadas podem estar na mesma conta ou em contas diferentes, mas devem estar na mesma região.

- Se você quiser conectar VPCs em regiões diferentes, use **Cloud Connect**.
- Você pode usar conexões de emparelhamento de VPC para criar redes diferentes. Para obter detalhes, consulte **Exemplos de uso de conexão de emparelhamento de VPC**.

Figura 10-4 mostra um cenário de aplicação de conexões de emparelhamento de VPC.

- Há duas VPCs (VPC-A e VPC-B) na região A que não são conectados.
- Os servidores de serviço (ECS-A01 e ECS-A02) estão no VPC-A e os servidores de banco de dados (RDS-B01 e RDS-B02) estão no VPC-B. Os servidores de serviço e os servidores de banco de dados não podem se comunicar uns com os outros.
- Você precisa criar uma conexão de emparelhamento de VPC (emparelhamento-AB) entre a VPC-A e a VPC-B para que os servidores de serviço e os servidores de banco de dados possam se comunicar uns com os outros.

Figura 10-4 Diagrama de rede de conexão de emparelhamento de VPC



10.6 ACLs da rede

A ACL da rede is an optional layer of security for your subnets. After you associate one or more subnets with a ACL da rede, you can control traffic in and out of the subnets.

Similar to security groups, ACLs da rede control access to subnets and add an additional layer of defense to your subnets. Security groups only have the "allow" rules, but ACLs da rede have both "allow" and "deny" rules. You can use ACLs da rede together with security groups to implement comprehensive and fine-grained access control.

ACLs da rede Basics

- Your VPC does not come with a ACLs da rede, but you can create a ACLs da rede and associate it with a VPC subnet if required. By default, each ACLs da rede denies all inbound traffic to and outbound traffic from the associated subnet until you add rules.
- You can associate a ACLs da rede with multiple subnets. However, a subnet can only be associated with one ACLs da rede at a time.
- Each newly created ACLs da rede is in the **Inactive** state until you associate subnets with it.
- ACLs da rede are stateful. If the ACLs da rede allows outbound traffic and you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound ACLs da rede rules. Similarly, if inbound traffic is allowed, responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

  The timeout period of connection tracking varies according to the protocol. The timeout period of a TCP connection in the established state is 600s, and the timeout period of an ICMP connection is 30s. For other protocols, if packets are received in both directions, the connection tracking timeout period is 180s. If one or more packets are received in one direction but no packet is received in the other direction, the connection tracking timeout period is 30s. For protocols other than TCP, UDP, and ICMP, only the IP address and protocol number are tracked.

Default regra de ACLs da rede

By default, each ACLs da rede has preset rules that allow the following packets:

- Packets whose source and destination are in the same subnet.
- Broadcast packets with the destination 255.255.255.255/32, which is used to configure host startup information.

- Multicast packets with the destination 224.0.0.0/24, which is used by routing protocols.
- Metadata packets with the destination 169.254.169.254/32 and TCP port number 80, which is used to obtain metadata.
- Packets from CIDR blocks that are reserved for public services (for example, packets with the destination 100.125.0.0/16).
- A ACLs da rede denies all traffic in and out of a subnet excepting the preceding packets. **Tabela 10-3** shows the default rules. You cannot modify or delete the default rules.

Tabela 10-3 Default regra de ACLs da rede

Direction	Priority	Action	Protocol	Source	Destination	Description
Inbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all inbound traffic.
Outbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all outbound traffic.

Rule Priorities

- Each ACLs da rede rule has a priority value where a smaller value corresponds to a higher priority. Any time two rules conflict, the rule with the higher priority is the one that gets applied. The rule whose priority value is an asterisk (*) has the lowest priority.
- If multiple regra de ACLs da rede conflict, only the rule with the highest priority takes effect. If you need a rule to take effect before or after a specific rule, you can insert that rule before or after the specific rule.

Application Scenarios

- If the application layer needs to provide services for users, traffic must be allowed to reach the application layer from all IP addresses. However, you also need to prevent illegal access from malicious users.

  Solution: You can add regra de ACLs da rede to deny access from suspect IP addresses.
- How can I isolate ports with identified vulnerabilities? For example, how do I isolate port 445 that can be exploited by WannaCry worm?

  Solution: You can add regra de ACLs da rede to deny access traffic from a specific port and protocol, for example, TCP port 445.
- No defense is required for the communication within a subnet, but access control is required for communication between subnets.

  Solution: You can add regra de ACLs da rede to control traffic between subnets.
- For frequently accessed applications, a security rule sequence may need to be adjusted to improve performance.

  Solution: A ACLs da rede allows you to adjust the rule sequence so that frequently used rules are applied before other rules.

10.7 Endereço IP virtual

Um endereço IP virtual pode ser compartilhado entre múltiplos ECSs. Um ECS pode ter endereços IP privados e virtuais, e você pode acessar o ECS por meio de qualquer endereço IP. Um endereço IP virtual tem os mesmos recursos de acesso à rede que um endereço IP privado, incluindo comunicação de camada 2 e camada 3 em VPCs, acesso entre VPCs usando conexões de emparelhamento de VPC, bem como acesso por meio de EIPs, conexões de VPN e conexões Direct Connect.

Você pode vincular ECSs implementados no modo ativo/em espera com o mesmo endereço IP virtual e, em seguida, vincular um EIP ao endereço IP virtual. Os endereços IP virtuais podem trabalhar em conjunto com o Keepalived para garantir alta disponibilidade e recuperação de desastres. Se o ECS ativo estiver com defeito, o ECS em espera assumirá automaticamente os serviços do ativo.

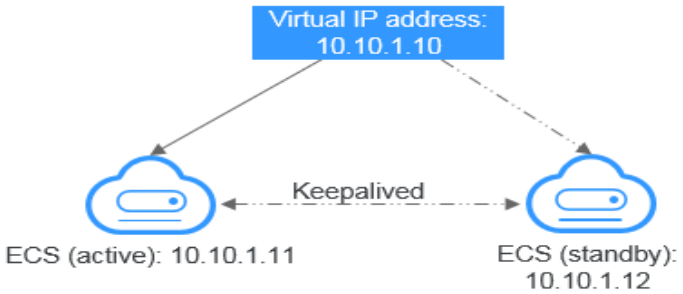
Rede

Os endereços IP virtuais são usados para alta disponibilidade e podem trabalhar em conjunto com o Keepalived para tornar possível a alternância do ECS ativo/em espera. Dessa forma, se um ECS for desativado por algum motivo, o outro poderá assumir o controle e os serviços continuarão ininterruptos. Os ECSs podem ser configurados para alta disponibilidade ou como clusters de balanceamento de carga.

- **Modo de rede 1**: alta disponibilidade

  Se você quiser melhorar a disponibilidade do serviço e evitar pontos únicos de falha, poderá implementar ECSs no modo ativo/em espera ou implementar um ECS ativo e vários ECSs em espera. Nesse arranjo, todos os ECSs usam o mesmo endereço IP virtual. Se o ECS ativo se tornar defeituoso, um ECS em espera assumirá os serviços do ECS ativo e os serviços continuarão ininterruptos.

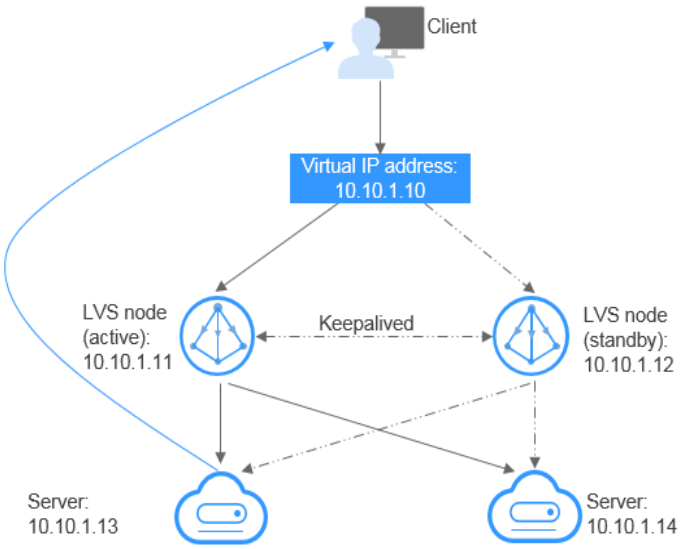
  Figura 10-5 Diagrama de rede do modo de alta disponibilidade

  - Nessa configuração, um único endereço IP virtual é vinculado a dois ECSs na mesma sub-rede.
  - Em seguida, o Keepalived é usado para configurar os dois ECSs para funcionar no modo ativo/em espera. Siga os padrões do setor para configurar o Keepalived. Os detalhes não estão incluídos aqui.
- **Modo de rede 2**: cluster de balanceamento de carga de HA

  Se você quiser criar um cluster de balanceamento de carga de alta disponibilidade, use o Keepalived e configure os nós do LVS como roteadores diretos.

Figura 10-6 Cluster de balanceamento de carga de HA



- Vincule um único endereço IP virtual a dois ECSs.
- Configure os dois ECSs como nós do LVS funcionando como roteadores diretos e use o Keepalived para configurar os nós no modo ativo/em espera. Os dois ECSs encaminharão solicitações uniformemente para servidores back-end diferentes.
- Configure mais dois ECSs como servidores back-end.
- Desative a verificação de origem/destino para os dois servidores back-end.

Siga os padrões do setor para configurar o Keepalived. Os detalhes não estão incluídos aqui.

Cenários de aplicação

- Acesso ao endereço IP virtual por meio de um EIP

  Se a sua aplicação tiver requisitos de alta disponibilidade e precisar fornecer serviços pela Internet, é recomendável vincular um EIP a um endereço IP virtual.
- Uso de uma conexão de emparelhamento de VPN, Direct Connect ou VPC para acessar um endereço IP virtual

  Para garantir alta disponibilidade e acesso à Internet, use uma VPN para segurança e Direct Connect para uma conexão estável. A conexão de emparelhamento de VPC é necessária para que as VPCs na mesma região possam se comunicar entre si.

10.8 Interface de rede elástica

Uma interface de rede elástica (referida como interface de rede nesta documentação) é uma placa de rede virtual. Você pode criar e configurar interfaces de rede e anexá-las às suas instâncias (ECSs e BMSs) para obter configurações de rede flexíveis e altamente disponíveis.

Tipos de interface de rede

- Uma interface de rede primária é criada junto com uma instância por padrão, que não pode ser desanexada da sua instância.

- Você pode criar interfaces de rede de extensão, anexá-las a uma instância e desanexá-las da instância. O número de interfaces de rede de extensão que você pode anexar a um ECS varia de acordo com o flavor do ECS.

Cenários de aplicação

- Migração flexível

  Você pode desanexar uma interface de rede de uma instância e, em seguida, anexá-la a outra instância. A interface de rede mantém seu endereço IP privado, EIP e regras de grupo de segurança. Dessa forma, o tráfego de serviço na instância defeituosa pode ser migrado rapidamente para a instância em espera, implementando a recuperação rápida do serviço.

- Gerenciamento de tráfego

  Você pode anexar várias interfaces de rede que pertencem a diferentes sub-redes em uma VPC à mesma instância e configurar as interfaces de rede para transportar o tráfego de rede privada, o tráfego de rede pública e o tráfego de rede de gerenciamento da instância. Você pode configurar políticas de controle de acesso e políticas de roteamento para cada sub-rede e configurar regras de grupo de segurança para cada interface de rede para isolar redes e tráfego de serviço.

Observações e restrições

- Uma instância e suas interfaces de rede de extensão devem estar na mesma AZ, VPC e sub-rede. No entanto, elas podem pertencer a diferentes grupos de segurança.

  NOTA

  Uma interface de rede criada usando a API pode estar em uma VPC diferente daquela da sua instância.

- Uma interface de rede primária não pode ser desanexada da sua instância.
- O número de interfaces de rede de extensão que você pode anexar a uma instância varia de acordo com o flavor da instância. Para obter detalhes, consulte **Especificações do ECS**.
- Interfaces de rede elásticas e NICs de extensão não podem ser usadas para acessar diretamente os serviços da Huawei Cloud, como o DNS. Você pode usar o VPCEP para acessar esses serviços. Para obter detalhes, consulte **Compra de um ponto de extremidade da VPC**.

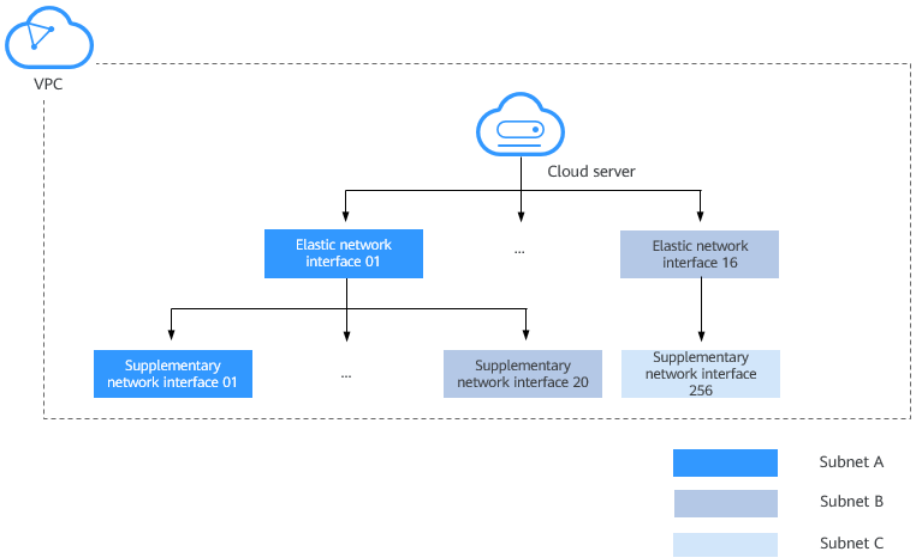
10.9 Interface de rede suplementar

Interfaces de rede suplementares são um complemento para interfaces de rede elásticas. Se o número de interfaces de rede elásticas que podem ser anexadas ao seu ECS não puder atender aos seus requisitos, você poderá usar interfaces de rede suplementares, que podem ser anexadas a subinterfaces VLAN de interfaces de rede elásticas.

Cenários de aplicação

As interfaces de rede suplementares são anexadas às subinterfaces VLAN de interfaces de rede elásticas. **Figura 10-7** mostra o diagrama de rede.

Figura 10-7 Diagrama de rede suplementar da interface de rede



O número de interfaces de rede elásticas que podem ser anexadas a cada ECS é limitado. Se esse limite não puder atender aos seus requisitos, você poderá anexar interfaces de rede suplementares a interfaces de rede elásticas.

- Você pode anexar interfaces de rede suplementares que pertençam a diferentes sub-redes na mesma VPC a um ECS. Cada interface de rede suplementar tem seu endereço IP privado e EIP para comunicação privada ou pela Internet.
- Você pode regras de grupo de segurança para interfaces de rede suplementares para isolamento de rede.

Observações e restrições

- Um máximo de 256 interfaces de rede suplementares podem ser anexadas a um ECS de determinados flavors. O número de interfaces de rede suplementares que podem ser anexadas a um ECS varia de acordo com o flavor do ECS. As especificações do ECS que suportam interfaces de rede suplementares são as seguintes:

  ECS: séries C7, S7 e M7. Para obter detalhes, consulte **Especificações do ECS**.

  Contêiner de nuvem: c6ne
- As interfaces de rede suplementares e sua interface de rede elástica devem estar na mesma VPC, mas podem pertencer a diferentes sub-redes e grupos de segurança.
- Atualmente, somente o grupo de segurança associado a uma interface de rede suplementar pode ser alterado.
- Os logs de fluxo da VPC de uma interface de rede suplementar são gerados junto com sua interface de rede elástica anexada.
- Antes de usar uma interface de rede suplementar, você precisa criar uma subinterface VLAN em sua NIC do ECS e configurar rotas.
- Um ECS não pode usar o Cloud-Init por meio dos endereços IP privados de suas interfaces de rede suplementares.
- Uma interface de rede suplementar não pode ter um endereço IP virtual vinculado.

10.10 Grupo de endereços IP

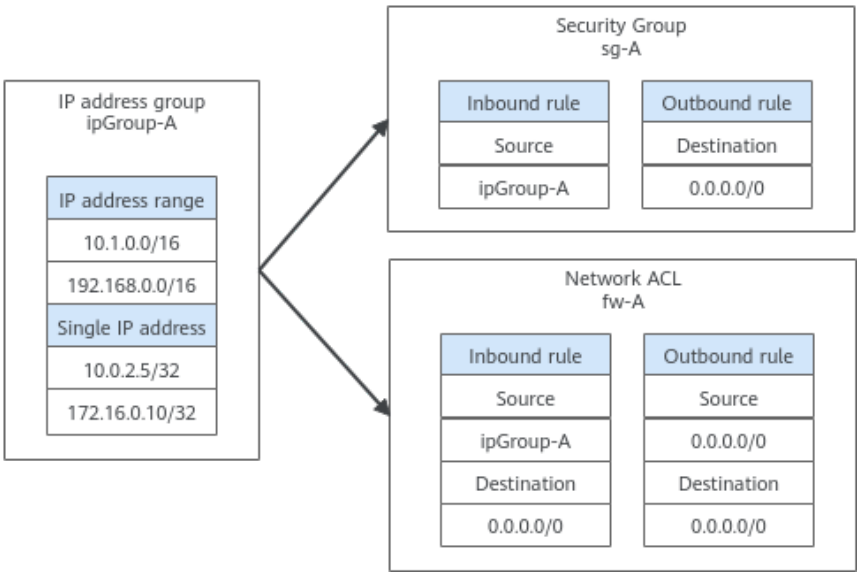
Um grupo de endereços IP é uma coleção de endereços IP. Ele pode ser associado a grupos de segurança e ACLs da rede para simplificar a configuração e o gerenciamento de endereços IP.

Você pode adicionar intervalos de endereços IP e endereços IP que precisam ser gerenciados de maneira unificada a um grupo de endereços IP. Um grupo de endereços IP pode trabalhar em conjunto com diferentes recursos de nuvem. **Tabela 10-4** lista os recursos que podem ser associados a um grupo de endereços IP.

Tabela 10-4 Recursos que podem ser associados a um grupo de endereços IP

Recurso	Descrição	Exemplo
Grupo de segurança	**Source** ou **Destination** de uma regra de grupo de segurança pode ser definida como **IP address group**.	Conforme mostrado em **Figura 10-8**, a regra de entrada do grupo de segurança sg-A usa o grupo de endereços IP ipGroup-A como origem.
ACL da rede	A **Source** ou o **Destination** de uma ACL da rede é definido como **IP address group**.	Conforme mostrado em **Figura 10-8**, a regra de entrada da ACL da rede fw-A usa o grupo de endereços IP ipGroup-A como origem.

Figura 10-8 Usar o grupo de endereços IP



10.11 Região e AZ

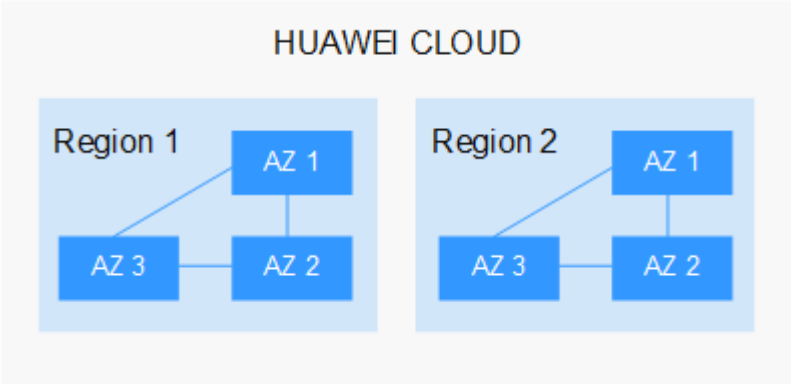
Conceito

Uma região e uma zona de disponibilidade (AZ) identificam a localização de um centro de dados. Você pode criar recursos em uma região e AZ específicas.

- As regiões são divididas com base na localização geográfica e na latência da rede. Serviços públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), são compartilhados na mesma região. As regiões são classificadas em regiões universais e regiões dedicadas. Uma região universal fornece serviços de nuvem universal para locatários comuns. Uma região dedicada fornece serviços específicos para locatários específicos.
- Uma AZ contém um ou mais centros de data físicos. Cada AZ possui resfriamento, sistema de extinção de incêndio, proteção contra umidade e instalações elétricas independentes. Dentro de uma AZ, computação, rede, armazenamento e outros recursos são logicamente divididos em vários clusters. As AZs dentro de uma região são interconectadas usando fibras ópticas de alta velocidade, para suportar sistemas de alta disponibilidade entre AZs.

Figura 10-9 mostra a relação entre regiões e AZs.

Figura 10-9 Regiões e as AZs



HUAWEI CLOUD fornece serviços em muitas regiões do mundo. Selecione uma região e uma AZ com base nos requisitos. Para obter mais informações, consulte **Regiões globais do Huawei Cloud**.

Selecionar uma região

Ao selecionar uma região, considere os seguintes fatores:

- Localização

  É recomendável selecionar a região mais próxima para menor latência de rede e acesso rápido. As regiões dentro do continente chinês fornecem a mesma infraestrutura, qualidade de rede BGP, bem como operações e configurações de recursos. Portanto, se seus usuários-alvo estiverem no continente chinês, você não precisará considerar as diferenças de latência da rede ao selecionar uma região.

  – Se seus usuários-alvo estiverem na Ásia-Pacífico (excluindo o continente chinês), selecione a região **CN-Hong Kong**, **AP-Bangkok**, ou **AP-Singapore**.
  – Se seus usuários-alvo estão na África, selecione a região **AF-Johannesburg**.
  – Se seus usuários de destino estiverem na América Latina, selecione a região **LA-Santiago**.

  NOTA

  A região **LA-Santiago** está localizada no Chile.

- Preço do recurso

  Os preços dos recursos podem variar em diferentes regiões. Para obter detalhes.

Selecionar uma AZ

Ao implantar recursos, considere os requisitos de recuperação de desastres (DR) e latência de rede de seus aplicativos.

- Para alta capacidade de DR, implante recursos nas diferentes AZs dentro da mesma região.
- Para menor latência de rede, implante recursos na mesma AZ.

Regiões e endpoints

Antes de usar uma API para chamar recursos, especifique sua região e endpoint. Para obter mais detalhes, consulte Regions and Endpoints.

