

Domain Name Service

Visão geral de serviço

Edição 01
Data 2024-04-30



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. Todos os direitos reservados.

Nenhuma parte deste documento pode ser reproduzida ou transmitida em qualquer forma ou por qualquer meio sem consentimento prévio por escrito da Huawei Cloud Computing Technologies Co., Ltd.

Marcas registadas e permissões



HUAWEI e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd.

Todas as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

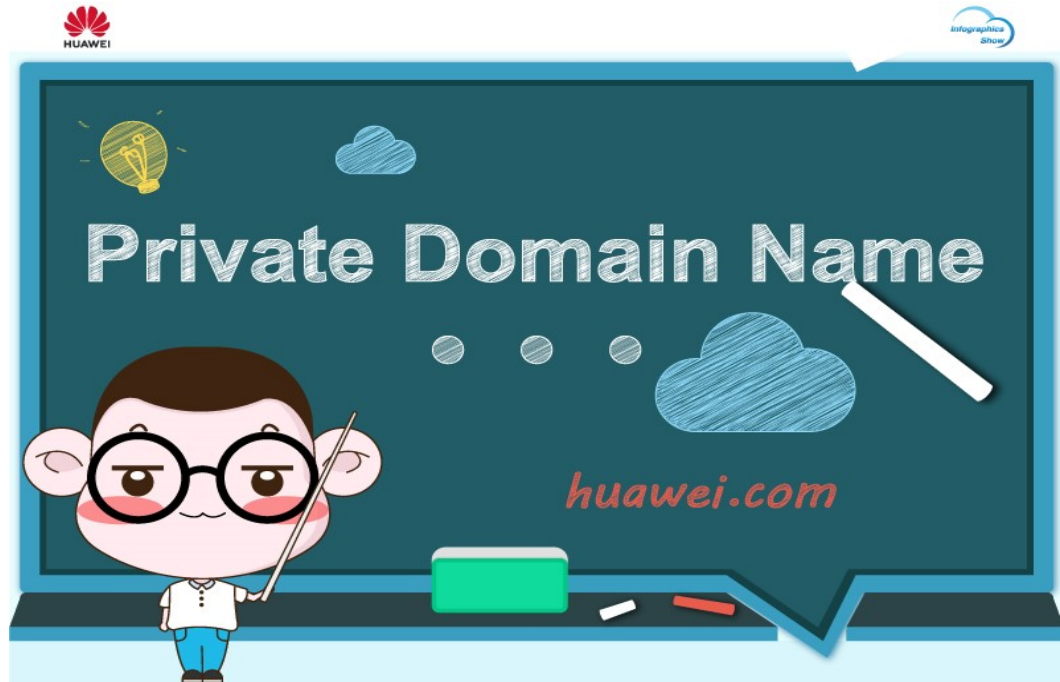
Os produtos, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo 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.

Índice

1 Infográficos do DNS.....	1
2 Infográficos do DNS.....	3
3 O que é o DNS?.....	5
4 Resolução de nome de domínio público.....	7
5 Resolução de nome de domínio privado.....	10
6 Resolução reversa.....	14
7 Resolução inteligente.....	15
8 Funções.....	16
9 Segurança.....	20
9.1 Responsabilidades compartilhadas.....	20
9.2 Identidade e controle de acesso.....	21
9.3 Auditoria e regisração.....	21
9.4 Resiliência.....	21
9.5 Monitoramento de riscos de segurança.....	22
9.6 Certificados.....	22
10 Gerenciamento de permissões.....	24
11 Integração com outros serviços.....	28
12 Conceitos de produto.....	30
12.1 Formato de nome de domínio e hierarquia do DNS.....	30
12.2 Conjunto de registros.....	30
12.3 Região e AZ.....	33
12.4 Projeto.....	34
13 Histórico de alterações.....	35

1 Infográficos do DNS



Preface

The DNS service offers private domain names for you to configure your own authoritative DNS servers in VPCs. By doing so, you can improve DNS resolution efficiency, reduce network latency, and prevent your private domain names from exposing to DNS spoofing on the Internet.

What Are Private Domain Names?

You can consider them as virtual domain names that only work in associated VPCs.



How a Private Domain Name Is Resolved?

Private domain names are applicable only to ECSs in specified VPCs. If you try to query a private domain name in an ECS, the private network DNS server will directly return you the resolution result. If you send a request to query a public domain name, the private network DNS server will forward the request to the public network for resolution.



2 Infográficos do DNS



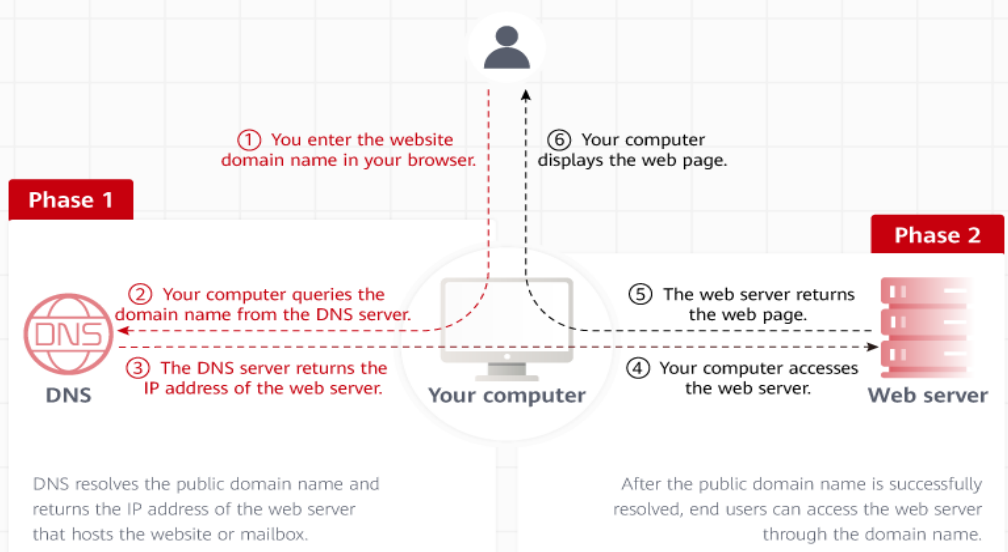
Public Domain Name



A public zone contains information about how a domain name and its subdomains are translated into IP addresses for routing traffic over the Internet.

Huawei Cloud Domain Name Service (DNS) allows end users to access your websites or email servers over the Internet using your domain names.

How Can I Access a Website or Mailbox Through a Domain Name?



How Do I Configure Public Domain Name Resolution?

3 O que é o DNS?

O Domain Name Service (DNS) é um serviço do DNS altamente disponível e escalável que converte nomes de domínio (como `www.example.com`) em endereços IP (como `192.1.2.3`) necessários para conexão de rede. O serviço do DNS permite que os usuários visitem seus sites ou aplicativos da web com nomes de domínio.

O serviço do DNS é gratuito e está ativado por padrão.

Funções básicas

O serviço do DNS fornece as seguintes funções:

- **Resolução de nome de domínio público**
Mapeia nomes de domínio para endereços IP públicos para que seus usuários possam acessar seu site ou aplicação da Web pela internet.
- **Resolução de nome de domínio privado**
Traduz nomes de domínio privados em endereços IP privados para facilitar o acesso a recursos de nuvem dentro de VPCs.
- **Resolução reversa**
Obtém um nome de domínio com base em um endereço IP. A resolução reversa, ou pesquisa reversa do DNS, é normalmente usada para afirmar a credibilidade dos servidores de e-mail.
- **Resolução inteligente**
Retorna resultados de resolução diferentes para o mesmo nome de domínio com base nas redes da operadora ou nas localizações geográficas dos endereços IP do usuário. Isso reduz significativamente a latência da rede para usuários de diferentes redes de operadoras e locais geográficos.

Vantagens do produto

O serviço do DNS tem as seguintes vantagens:

- **Alto desempenho**
Um único nó do DNS pode lidar com milhões de consultas simultâneas, permitindo que os usuários finais acessem seu site ou aplicativo mais rapidamente.
- **Fácil acesso aos recursos da nuvem**

Seus ECSs podem se comunicar uns com os outros e com outros recursos dentro das VPCs usando nomes de domínio privados. O tráfego é mantido dentro de sua rede interna, o que reduz a latência da rede e melhora a segurança.

Para obter mais detalhes, consulte [Configuração de um nome de domínio privado para um ECS](#).

- Migração de serviço perfeito
Você pode migrar um nome de domínio de site em uso para o serviço do DNS da Huawei Cloud. Para garantir que os serviços do seu site não sejam interrompidos durante a migração, criaremos uma zona pública e adicionaremos conjuntos de registros do DNS para o seu site com antecedência.
- Isolamento dos dados principais
Um servidor do DNS privado fornece resolução de nomes de domínio para ECSs que carregam dados principais, permitindo acesso seguro e controlado a esses dados. Não é necessário vincular EIPs a esses ECSs.

Acessando o serviço do DNS

A plataforma em nuvem fornece um console de gerenciamento baseado na Web, bem como APIs REST por meio das quais você pode acessar o serviço do DNS.

- Console de gerenciamento
Um console de gerenciamento baseado na Web permite que você acesse o serviço do DNS.
 - Se você já registrou uma conta, faça login no console de gerenciamento, passe o mouse sobre a parte superior esquerda para exibir **Service List** e escolha **Networking > Domain Name Service**.
 - Caso contrário, registre uma conta na Huawei Cloud seguindo as instruções no [Início rápido](#) e execute o passo anterior.

Com algumas etapas, você pode começar a usar o serviço do DNS para resolução de nomes de domínio.

- As API
As APIs REST são fornecidas para acessar o serviço do DNS. Você também pode usar as APIs fornecidas para integrar o DNS a um sistema de terceiros para desenvolvimento secundário. Para obter detalhes, consulte a [Referência de API do Domain Name Service](#).

4 Resolução de nome de domínio público

Zona pública

Uma zona pública contém informações sobre como um nome de domínio e seus subdomínios são traduzidos em endereços IP para roteamento de tráfego pela Internet. Isso permite que os usuários finais acessem seu site ou aplicativo pela Internet usando seu nome de domínio.

Acesso a um site usando um nome de domínio

Para tornar seu site acessível na Internet por meio de um nome de domínio, execute as seguintes etapas:

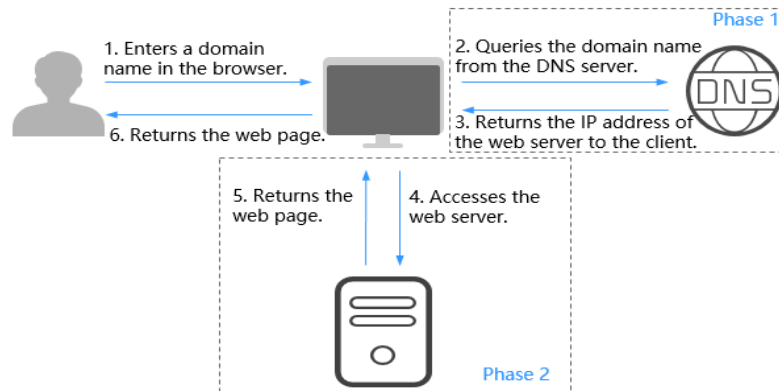
1. Registre seu nome de domínio com um registrador de nomes de domínio para que seus usuários possam usá-lo para acessar seu site.
2. Configure o seu site.
Compre recursos de nuvem da Huawei Cloud ou de outro provedor de nuvem.
3. Configure o serviço do DNS para rotear o tráfego da Internet para o seu nome de domínio.

Crie uma zona pública para hospedar o nome de domínio no serviço do DNS e adicione um conjunto de registros para mapear o nome de domínio para o EIP do servidor onde o site está configurado.

Para obter detalhes, consulte [Roteamento de tráfego da internet para um site](#).

Depois de concluir as etapas acima, os usuários finais poderão acessar seu site pela Internet com o nome de domínio registrado e seus subdomínios.

Figura 4-1 Como o DNS direciona o tráfego da internet para um site



- A fase 1 mostra como o DNS resolve seu nome de domínio.
- A fase 2 mostra como um usuário acessa seu site usando seu nome de domínio.

A resolução de nomes de domínio público depende da hierarquia de DNS. O seguinte descreve as hierarquias de nomes de domínio e como os nomes de domínio são resolvidos.

Hierarquia do DNS

Os nomes de domínio são hierárquicos e a resolução de domínio é um processo de pesquisa recursivo. O seguinte usa `example.com` para descrever as hierarquias em nomes de domínio.

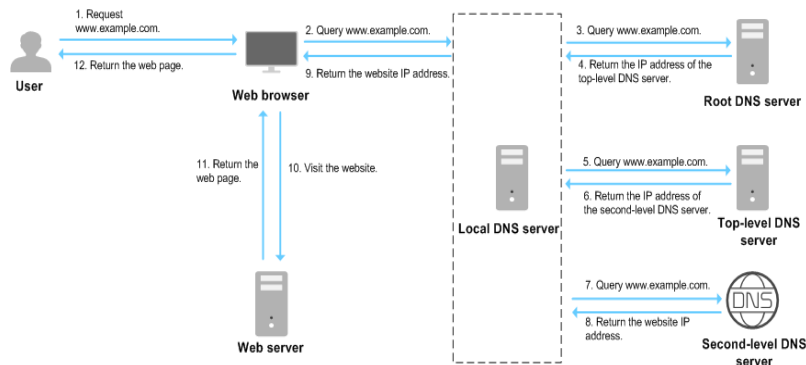
- Domínio raiz
Um período (.) é a designação para o domínio raiz.
Um nome de domínio totalmente qualificado (FQDN) termina com um ponto (`exemplo.com.`). Quando você insere um nome de domínio (`exemplo.com`) no navegador, o sistema do DNS adicionará automaticamente um ponto final.
Os nomes de domínio raiz são resolvidos por servidores do DNS raiz que mantêm os endereços dos servidores do DNS de nível superior.
- Domínio de nível superior
Abaixo do domínio raiz estão os domínios de nível superior, categorizados em dois tipos:
 - Domínio de nível superior genérico (gTLD), como `.com`, `.net`, `.org` e `.top`
 - Domínio de topo com código de país (ccTLD), como `.cn`, `.uk` e `.de`Os domínios de nível superior são resolvidos por servidores do DNS de nível superior que contêm os endereços dos servidores do DNS de segundo nível. Por exemplo, o servidor do DNS de nível superior de `com` salva os endereços de todos os servidores do DNS de nomes de domínio de segundo nível que terminam com `com`.
- Domínio de segundo nível
Os domínios de segundo nível (como `example.com`) são subdomínios de domínios de nível superior e são resolvidos por servidores do DNS de segundo nível, que fornecem serviços de resolução de nomes de domínio autoritativos.
Por exemplo, se você comprar `example.com` de um registrador de nomes de domínio e definir um servidor do DNS para o nome de domínio, o servidor do DNS fornecerá resolução autoritativa para `example.com` e seu endereço será registrado por todos os servidores do DNS de nível superior.

Se você hospedar nomes de domínio no serviço DNS da Huawei Cloud, servidores de DNS autoritativos serão fornecidos para os nomes de domínio.

Resolução do nome de domínio

Figura 4-2 mostra o processo para acessar um site usando o nome de domínio `www.example.com`.

Figura 4-2 Resolução do nome de domínio



1. Um usuário digita **www.example.com** na caixa de endereço do navegador.
2. A solicitação de consulta de nome de domínio `www.example.com` é então enviada para o servidor do DNS local.

Os servidores do DNS locais são geralmente fornecidos pelo provedor de serviços de Internet para armazenar em cache as informações do nome de domínio e realizar pesquisas recursivas.

3. Se o servidor do DNS local não encontrar nenhum registro no cache, ele encaminha a solicitação de `www.example.com` para o servidor do DNS raiz.
4. O servidor do DNS raiz retorna o endereço de servidor do DNS `of.com` (porque o sufixo de nome de domínio é `.com`) para o servidor do DNS local.
5. O servidor do DNS local envia o pedido de consulta para o servidor do DNS `of.com`.
6. O servidor do DNS `.com` retorna o endereço do servidor do DNS de segundo nível que fornece registros autoritativos para `example.com`.
7. O servidor do DNS local envia a solicitação para o servidor do DNS de `example.com`.
8. O servidor do DNS de segundo nível retorna o endereço IP mapeado para `www.example.com` para o servidor do DNS local.
9. O servidor do DNS local retorna o endereço IP para o navegador da Web.
10. O navegador da Web acessa o servidor do site com o endereço IP.
11. O servidor do site retorna a página da Web para o navegador.
12. O usuário visualiza a página da Web usando o navegador.

Para obter detalhes, consulte [Roteamento de tráfego da internet para um site](#).

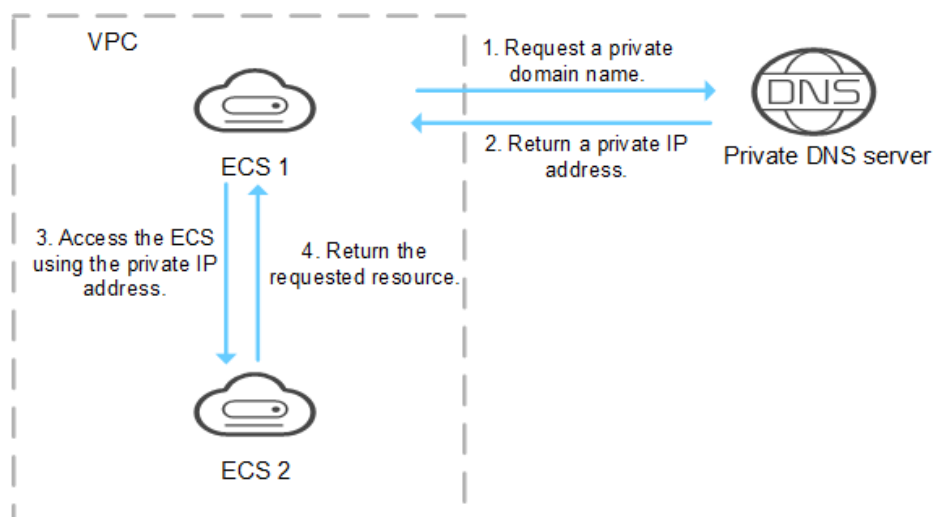
5 Resolução de nome de domínio privado

Zona privada

Uma zona privada contém informações sobre como mapear um nome de domínio (como `ecs.com`) e seus subdomínios usados em uma ou mais VPCs para endereços IP privados (como `192.168.1.1`). Com nomes de domínio privados, seus ECSs podem se comunicar entre si dentro das VPCs sem precisar se conectar à internet. Esses ECSs também podem acessar serviços em nuvem, como OBS e SMN, em uma rede privada.

Figura 5-1 mostra como um nome de domínio privado é resolvido por um servidor do DNS privado.

Figura 5-1 Processo para resolver um nome de domínio privado



Quando um ECS na VPC solicita um nome de domínio privado, o servidor do DNS privado retorna diretamente um endereço IP privado mapeado para o nome de domínio.

As zonas privadas permitem que você:

- personalize com flexibilidade nomes de domínio privados em suas VPCs.
- associe uma ou mais VPCs a um nome de domínio.

- use servidores do DNS privados para impedir a falsificação de DNS e responda rapidamente a solicitações de acesso a ECSs em VPCs, bem como a recursos OBS e SMN.

Você pode usar nomes de domínio privados nos seguintes cenários:

- **Gerenciamento de nomes de host do ECS**
- **Mantimento de seu site funcionando mesmo enquanto seu servidor está sendo substituído**
- **Acesso aos recursos da nuvem**

Gerenciamento de nomes de host do ECS

Você pode planejar nomes de host com base nos locais, usos e informações de conta dos ECSs e mapear os nomes de host para endereços IP privados, ajudando a gerenciar ECSs com mais facilidade.

Por exemplo, se você implantou 20 ECSs em uma AZ, 10 para o site A e 10 para o site B, é possível planejar seus nomes de host (nomes de domínio privados) da seguinte maneira:

- ECSs para o site A: weba01.region1.az1.com – weba10.region1.az1.com
- ECSs para o site B: webb01.region1.az1.com – webb10.region1.az1.com

Depois de configurar os nomes de host, você poderá determinar rapidamente os locais e os usos dos ECSs durante o gerenciamento e a manutenção de rotina.

Consulte [Roteamento de tráfego nas VPCs](#) para obter operações detalhadas.

Mantimento de seu site funcionando mesmo enquanto seu servidor está sendo substituído

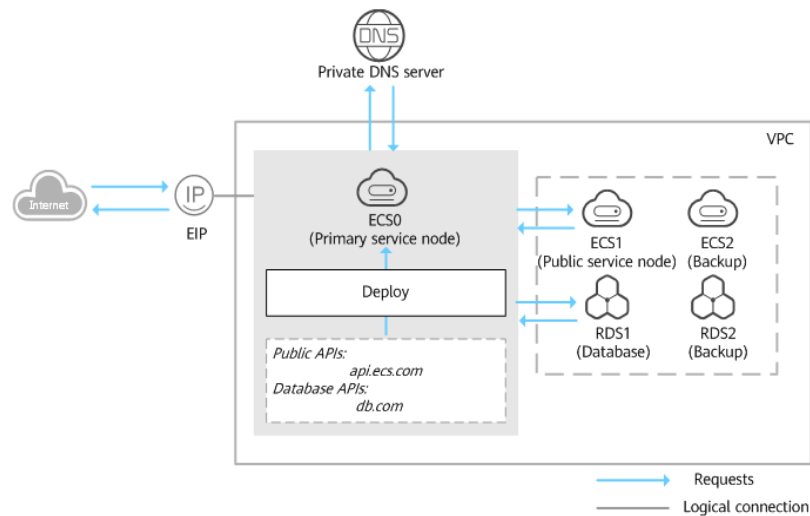
Como o número de usuários da internet está aumentando continuamente, um site ou aplicação da Web implantado em um único servidor dificilmente pode lidar com solicitações simultâneas durante as horas de pico. Uma prática comum é implantar o site ou aplicativo em vários servidores e distribuir a carga entre os servidores.

Esses servidores estão na mesma VPC e se comunicam entre si usando endereços IP privados codificados em APIs internas chamadas entre os servidores. Se um desses servidores for substituído, seu endereço IP privado será alterado. Como resultado, você precisa alterar esse endereço IP nas APIs e publicar novamente o site. Isso apresenta desafios para a manutenção do sistema.

Se você criar uma zona privada para cada servidor e configurar conjuntos de registros para mapear seus nomes de domínio privados para os endereços IP privados, eles poderão se comunicar usando nomes de domínio privados. Quando você substitui qualquer um dos servidores, você só precisa alterar o endereço IP privado no conjunto de registros, em vez de modificar o código.

Figura 5-2 ilustra esse uso de resolução de nomes de domínio privado.

Figura 5-2 Configuração do DNS privado para servidores em nuvem



As instâncias ECSs e RDS estão na mesma VPC.

- ECS0: nó de serviço principal
- ECS1: nó de serviço público
- RDS1: base de dados de serviços
- ECS2 e RDS2: nó de serviço de backup e banco de dados de backup

Quando o ECS1 se torna defeituoso, o ECS2 deve assumir. No entanto, se nenhuma zona privada estiver configurada para os dois ECSs, você precisará alterar os endereços IP privados no código do ECS0. Isso interromperá os serviços e você precisará publicar o site novamente.

Agora, suponha que você configurou zonas privadas para os ECSs e incluiu seus nomes privados no código. Se o ECS1 se tornar defeituoso, você só precisará alterar os registros do DNS para direcionar o tráfego para o ECS2. Os serviços não são interrompidos e você não precisa publicar o site novamente.

Consulte [Configuração de um nome de domínio privado para um ECS](#) para obter operações detalhadas.

Acesso aos recursos da nuvem

Configure nomes de domínio privados para ECSs para que eles possam acessar outros serviços de nuvem, como o SMN e o OBS, sem se conectar à internet.

Ao criar um ECS, observe o seguinte:

- Se um servidor do DNS público estiver configurado para a sub-rede da VPC onde o ECS reside, as solicitações de acesso aos serviços em nuvem serão roteadas pela internet.

Figura 5-3 mostra o processo para resolver um nome de domínio quando um ECS acessa os serviços de nuvem da Huawei, como o OBS e o SMN.

As solicitações são roteadas pela internet, resultando em um aumento na latência da rede.

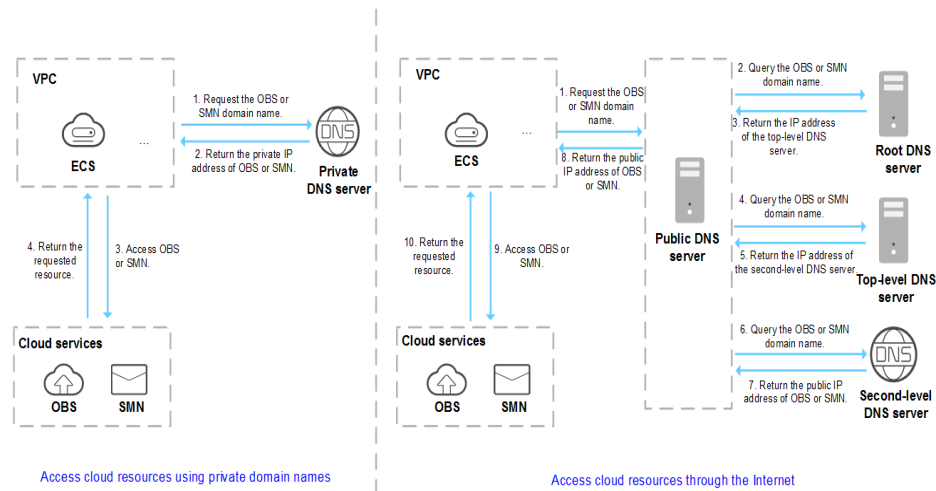
- Se um servidor do DNS privado estiver configurado para a sub-rede, o servidor do DNS privado processará diretamente as solicitações para acessar os serviços em nuvem.

Quando o ECS acessa os serviços de nuvem da Huawei, o servidor do DNS privado retorna seus endereços IP privados, em vez de rotear solicitações pela internet. Isso reduz

a latência da rede e melhora a velocidade de acesso. Passos 1 a 4 à esquerda de **Figura 5-3** mostra o processo.

Para tornar seu ECS acessível dentro da rede privada, altere os servidores do DNS padrão do ECS para servidores do DNS privados, consulte **Como fazer para alterar servidores do DNS padrão de um ECS para servidores do DNS privados fornecidos pelo serviço do DNS?**

Figura 5-3 Acesso aos serviços em nuvem



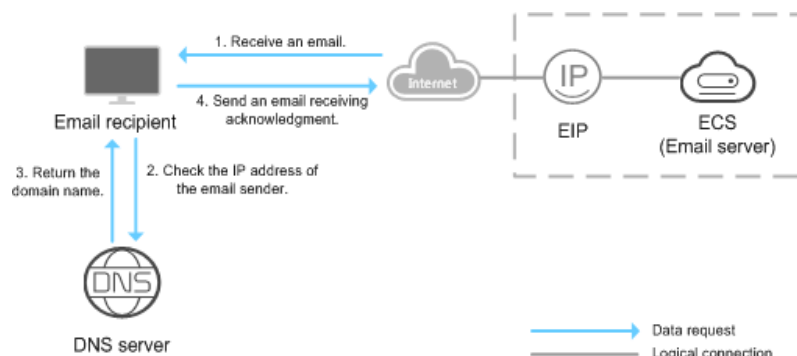
6 Resolução reversa

Resolução inversa significa obter um nome de domínio com base em um endereço IP. Isso é normalmente usado para afirmar a credibilidade dos servidores de e-mail.

Depois que um servidor de destinatário recebe um e-mail, ele verifica se o endereço IP e o nome de domínio do servidor remetente são confiáveis e determina se o e-mail é spam. Se o servidor destinatário não conseguir obter o nome de domínio mapeado para o endereço IP do servidor remetente, ele conclui que o e-mail é enviado por um host mal-intencionado e o rejeita. É necessário configurar registros de ponteiro (PTR) para apontar os endereços IP de seus servidores de e-mail para nomes de domínio.

Na figura a seguir, um ECS funciona como um servidor de e-mail e um registro PTR é configurado para mapear o EIP do ECS para o nome de domínio configurado para acessar o servidor de e-mail.

Figura 6-1 Resolução reversa



NOTA

Figura 6-1 mostra apenas o processo para resolução reversa. As informações sobre como um servidor de e-mail verifica a credibilidade do endereço IP do remetente e se o nome de domínio está disponível na Internet não são fornecidas aqui.

Se nenhum registro de PTR estiver configurado, o servidor do destinatário tratará os e-mails do servidor de e-mail como spam ou mal-intencionado e os descartará.

Consulte [Tradução de um endereço IP para um nome de domínio](#) para obter operações detalhadas.

7 Resolução inteligente

Normalmente, um servidor do DNS retorna o mesmo resultado de resolução para visitantes de diferentes redes ou locais geográficos. No entanto, no acesso entre redes ou entre regiões, isso levaria a um aumento na latência da rede e à má experiência do usuário.

Com linhas de resolução configuráveis, você pode especificar que o servidor do DNS retorne resultados de resolução diferentes para o mesmo nome de domínio com base nas redes ou localizações geográficas dos endereços IP dos visitantes.

Você pode criar linhas de resolução mais refinadas com base nos endereços IP de origem.

O DNS da Huawei Cloud suporta os seguintes tipos de linhas de resolução:

- **Linhas de ISP**
- **Linhas de região**

 **NOTA**

As linhas de resolução não estão disponíveis para zonas privadas e registros de PTR.

8 Funções

Tabela 8-1 lista as funções básicas do serviço do DNS.

Antes de usar o serviço do DNS, é melhor você se familiarizar com **Conceitos de produto** para entender melhor as funções.

Tabela 8-1 Funções comuns do DNS

Categoria	Função	Descrição
Resolução de domínio público	Zona pública	O DNS permite que você hospede nomes de domínio registrados com registradores de nomes de domínio e fornece serviços de resolução na internet para seus nomes de domínio. O DNS permite que você crie, modifique, exclua, habilite, desabilite e visualize zonas públicas. Para obter detalhes, consulte Zona pública .
	Nível de nome de domínio	O DNS permite que você crie zonas públicas para nomes de domínio de segundo nível e seus subdomínios. <ul style="list-style-type: none">● Para nomes de domínio com sufixos de 1 nível como .com, você pode criar zonas como example.com e www.example.com.● Para nomes de domínio com sufixos de 2 níveis como .com.cn, você pode criar zonas como exemplo.com.cn e www.example.com.cn.
	Conjunto de registros	Um conjunto de registros é um grupo de registros de recursos que definem o tipo de resolução e o valor de um nome de domínio. Você pode adicionar, modificar, excluir, exibir, desativar ou habilitar conjuntos de registros dos tipos A, CNAME, MX, AAAA, TXT, SRV, NS e CAA para zonas públicas. Para obter detalhes, consulte Conjunto de registros .

Categoria	Função	Descrição
	Recuperação de um nome de domínio	<p>Se uma zona pública tiver sido criada para o seu nome de domínio por outro utilizador, pode recuperar o nome de domínio provando a propriedade deste nome de domínio ao serviço do DNS.</p> <p>Para obter detalhes, consulte Recuperação de um nome de domínio.</p>
	Resolução de caracteres curinga	<p>Você pode adicionar conjuntos de registos para todos os subdomínios de um nome de domínio de segundo nível. O DNS fornece serviços de resolução para todos os subdomínios.</p> <p>Para obter detalhes, consulte Criação de um conjunto de registos DNS curinga.</p>
	TTL	<p>O TTL é curto para o tempo de vida, que especifica o período de cache de registos de recursos em um servidor do DNS local, em segundos. O valor do TTL varia de 300 a 2147483647.</p>
	Peso	<p>Peso indica a proporção de consultas do DNS que serão encaminhadas para o conjunto de registos.</p> <p>Se uma linha de resolução em uma zona contiver vários conjuntos de registos do mesmo tipo, você poderá definir pesos diferentes para cada conjunto de registos.</p> <p>Para obter detalhes, consulte Configuração do roteamento ponderado.</p>
	Exclusão em lote de zonas públicas	<p>Você pode excluir várias zonas públicas por vez.</p>
Resolução de domínio privado	Zona privada	<p>Você pode criar nomes de domínio privados que entram em vigor nas VPCs associadas. O DNS permite criar, modificar, excluir e exibir zonas privadas, associar zonas privadas a VPCs e desassociar zonas privadas das VPCs.</p> <ul style="list-style-type: none"> ● Zonas privadas podem ser criadas sem a necessidade de registrar nomes de domínio. ● A zona privada deve ser exclusiva na VPC associada. <p>Para obter detalhes, consulte Zona privada.</p>
	Associação ou desassociação de uma zona privada de uma VPC	<p>Você pode associar uma zona privada a uma VPC ou desassociar uma zona privada de uma VPC.</p> <p>Para obter detalhes, consulte Associação de uma VPC a uma zona privada e Desassociação de uma VPC de uma zona privada.</p>

Categoria	Função	Descrição
	Conjunto de registros	Um conjunto de registros é um grupo de registros de recursos que definem o tipo de resolução e o valor de um nome de domínio. Você pode adicionar, modificar, excluir ou exibir conjuntos de registros A, CNAME, MX, AAAA, TXT, PTR e SRV para zonas privadas. Para obter detalhes, consulte Conjunto de registros .
	Resolução de caracteres curinga	Você pode adicionar conjuntos de registros para todos os subdomínios de um nome de domínio privado. O DNS fornece serviços de resolução para todos os subdomínios. Para obter detalhes, consulte Criação de um conjunto de registros DNS curinga .
	TTL	O TTL é curto para o tempo de vida, que especifica o período de cache de registros de recursos em um servidor do DNS local, em segundos. O valor do TTL varia de 300 a 2147483647 .
	Exclusão em lote de zonas privadas	Você pode excluir várias zonas privadas de uma vez.
Resolução reversa	Registro de PTR	A resolução reversa envolve a obtenção de um nome de domínio com base em um endereço IP. Essa função é útil quando você deseja criar um servidor de e-mail. Você pode criar, modificar e excluir registros de PTR. Para obter detalhes, consulte Registro de PTR .
	TTL	O TTL é curto para o tempo de vida, que especifica o período de cache de registros de recursos em um servidor do DNS local, em segundos. O valor do TTL varia de 300 a 2147483647 .
Resolução inteligente	Linha de ISP	O DNS pode encaminhar os visitantes para o endereço ideal com base nas redes de operadoras que eles usam. Para obter detalhes, consulte Configuração de linhas de ISP .
	Linha de região	O DNS pode encaminhar os visitantes para o endereço ideal com base em suas localizações geográficas. Para obter detalhes, consulte Configuração de linhas de região .

Categoria	Função	Descrição
Conjunto de registros	Procura de conjuntos de registros globalmente	<p>O DNS permite que você gerencie centralmente conjuntos de registros em zonas públicas e privadas, incluindo o seguinte:</p> <ul style="list-style-type: none"> ● pesquisa de conjuntos de registros por status, tipo, nome, valor, ID ou tag ● modificação, exclusão, desabilitação ou habilitação de conjuntos de registros em zonas públicas ● modificação ou exclusão de conjuntos de registros de zonas privadas <p>Para obter detalhes, consulte Pesquisa de conjuntos de registros.</p>
	Exclusão em lote de zonas privadas	<p>Você pode importar, exportar e excluir conjuntos de registros em zonas públicas e privadas em lotes.</p> <p>Para obter detalhes, consulte Importação de conjuntos de registros e Exportação de conjuntos de registros.</p>
Auditoria	Visualização de registros de auditoria	<p>Com o CTS, você pode registrar operações associadas ao DNS para operações posteriores de consulta, auditoria e backtrack.</p> <p>A Huawei Cloud permite que você visualize e exporte registros de operação dos últimos sete dias no console do CTS.</p>
Tag	Tag de recurso	<p>Você pode configurar tags para zonas públicas, zonas privadas, conjuntos de registros e registros de PTR. Você também pode usar tags predefinidas do TMS para associar rapidamente tags a recursos.</p>
Cota	Ajuste de cota	<p>As cotas são impostas para recursos de serviço na plataforma para evitar picos imprevistos no uso de recursos. As cotas podem limitar o número e a capacidade de recursos disponíveis para os usuários, por exemplo, quantas zonas públicas, zonas privadas, conjuntos de registros e registros de PTR você pode criar.</p> <p>Se a cota de recursos existente não puder atender aos seus requisitos de serviço, você poderá solicitar uma cota mais alta.</p> <p>Para obter detalhes, consulte Ajuste de cota.</p>

9 Segurança

9.1 Responsabilidades compartilhadas

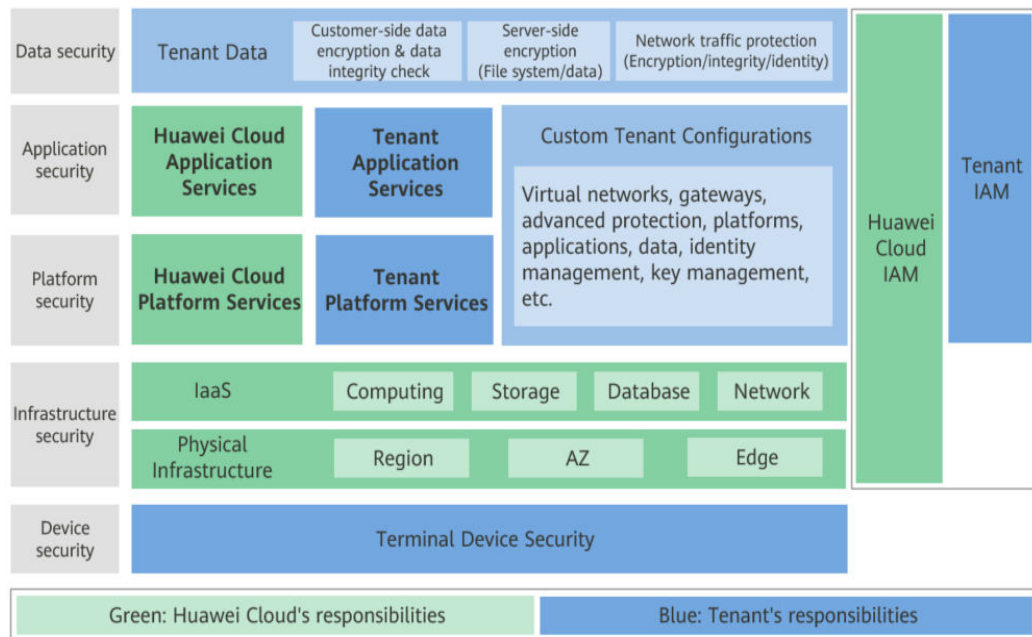
Huawei garante que seu compromisso com a segurança cibernética nunca será superado pela consideração de interesses comerciais. Para lidar com os desafios emergentes de segurança na nuvem e ameaças e ataques à segurança na nuvem, a Huawei Cloud constrói um sistema abrangente de garantia de segurança de 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 9-1 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 9-1 Modelo de responsabilidade de segurança compartilhada da Huawei Cloud



9.2 Identidade e controle de acesso

Você pode usar o Identity and Access Management (IAM) para controlar o acesso aos seus recursos do DNS. As permissões do IAM definem quais ações em seus recursos de nuvem são permitidas ou negadas. Depois de criar um usuário do IAM, o administrador precisa adicioná-lo a um grupo de usuários e conceder as permissões exigidas pelo DNS ao grupo de usuários. Em seguida, todos os usuários neste grupo herdam automaticamente as permissões concedidas.

Para obter detalhes, consulte [Gerenciamento de permissões](#).

9.3 Auditoria e registro

O Cloud Trace Service (CTS) é um serviço de auditoria de log para a segurança da Huawei Cloud. Ele permite que você colete, armazene e consulte registros de operação de recursos da nuvem. Você pode usar esses registros para realizar análises de segurança, auditar a conformidade, rastrear alterações de recursos e localizar falhas.

Depois que o CTS é habilitado, os rastros podem ser gerados para operações do DNS.

- Para obter detalhes sobre como habilitar e configurar o CTS, consulte [Habilitação do CTS](#).
- Para obter detalhes sobre as principais operações do DNS, consulte [Operações-chave gravadas pelo CTS](#).
- Para obter detalhes sobre rastros, consulte [Visualização de rastros](#).

9.4 Resiliência

Mais de 100 nós do DNS foram implantados em mais de 20 países e regiões em todo o mundo. O DNS fornece recuperação de desastres multi-AZ e multi-cluster em cada região,

portanto, mesmo que alguns nós, clusters ou regiões fiquem inativos, a resolução de nomes de domínio não será interrompida. O DNS fornece a confiabilidade do serviço com o qual você pode contar.

A Huawei tem mais de 10 anos de experiência em segurança da informação e tem uma riqueza de excelentes práticas nas quais confiar. Com base nas salas de equipamentos de alta segurança autoconstruídas da Huawei Cloud e nos centros de depuração de alta segurança nas redes de backbone das operadoras, o DNS fornece proteção de DDoS de nível Terabyte. Ele pode lidar de forma rápida e eficaz com vários ataques DNS para garantir a continuidade da resolução de nomes de domínio.

O Kit de Desenvolvimento de Plano de Dados (DPDK) de próxima geração da Huawei oferece maior desempenho de resolução. Com o DPDK, um único nó do DNS pode suportar dezenas de milhões de solicitações simultâneas, portanto, o DNS pode suportar centenas de milhões de solicitações simultâneas. Você obtém serviços de resolução de alto desempenho com escalabilidade ilimitada.

O DNS da Huawei suporta resolução inteligente. O tráfego de usuários é agendado automaticamente para diferentes servidores de back-end por operadora, continente/país ou peso, melhorando consideravelmente a confiabilidade do serviço.

9.5 Monitoramento de riscos de segurança

O Cloud Eye é um serviço de monitoramento da Huawei Cloud. Ele fornece recursos como monitoramento em tempo real, relatórios de alarme oportunos, grupos de recursos e monitoramento de sites. O Cloud Eye ajuda você a acompanhar seus usos de recursos e status de serviço na nuvem, facilitando a resposta a exceções em tempo hábil.

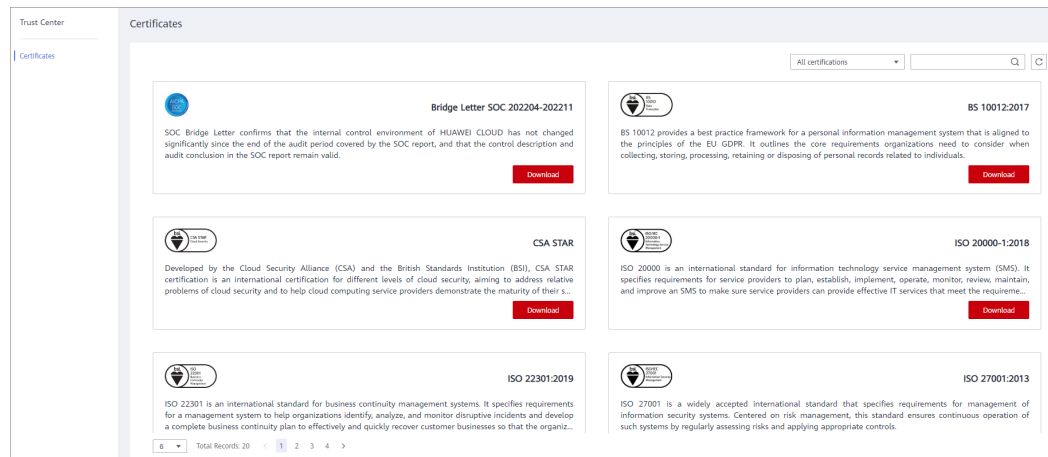
O monitoramento é fundamental para garantir a confiabilidade, a disponibilidade e o desempenho do serviço do DNS. Com o Cloud Eye, você pode visualizar o tráfego de resolução de nome de domínio e logs de erro dentro do período de tempo selecionado. Você também pode analisar dinamicamente os riscos potenciais com base nos alarmes gerados.

9.6 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). Você pode [baixá-los](#) do console.

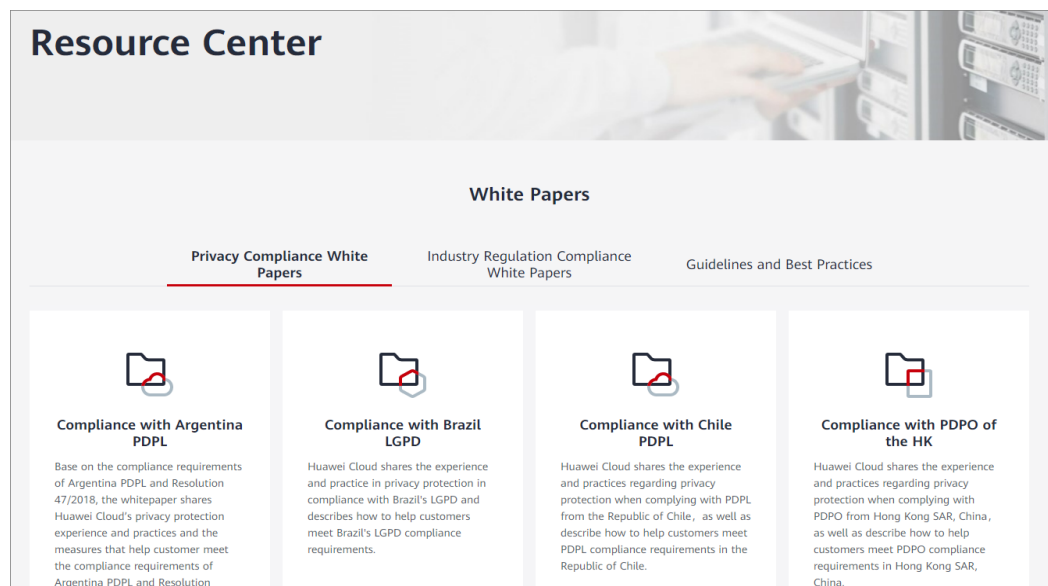
Figura 9-2 Download de certificados de conformidade



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 9-3 Central de recursos



10 Gerenciamento de permissões

Se você precisar atribuir permissões diferentes a funcionários em sua empresa para acessar seus recursos do DNS na Huawei Cloud, o IAM é adequado para o gerenciamento de permissões refinado. O IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a gerenciar com segurança o acesso aos seus recursos de nuvem da Huawei.

Com o IAM, você pode usar sua conta da Huawei Cloud para criar usuários do IAM e atribuir permissões aos usuários para controlar seu acesso a recursos específicos. Por exemplo, alguns desenvolvedores de software em sua empresa precisam usar recursos do DNS, mas não devem conseguir excluí-los ou executar outras operações de alto risco. Nesse cenário, você pode criar usuários do IAM para os desenvolvedores de software e conceder a eles apenas as permissões necessárias para o uso de recursos específicos.

Ignore esta parte se sua conta da Huawei Cloud não exigir usuários individuais do IAM para gerenciamento de permissões.

O IAM gratuito. Você paga apenas pelos recursos de nuvem que compra ou usa. Para obter mais informações sobre o IAM, consulte [O que é o IAM?](#)

Permissões do DNS

Por padrão, os novos usuários do IAM não têm nenhuma permissão atribuída. Para atribuir permissões a esses novos usuários, adicione-os a um ou mais grupos e anexe políticas de permissões ou funções a esses grupos. E pode executar operações especificadas em serviços de nuvem.

Os recursos do DNS incluem o seguinte:

- zona pública: recurso de nível global
- zona privada: recurso no nível do projeto
- registro de PTR: recurso no nível do projeto

As permissões do DNS para recursos de nível global não podem ser definidas no projeto de serviço global e devem ser concedidas para cada projeto.

Para atribuir permissões do DNS a um grupo de usuários, especifique o escopo como projetos específicos da região e selecione os projetos para que as permissões entrem em vigor. Se **All projects** estiver selecionado, as permissões entrarão em vigor para o grupo de usuários em todos os projetos específicos da região. Ao acessar o serviço do DNS, os usuários precisam mudar para uma região onde foram autorizados a usar recursos DNS.

Você pode conceder permissões aos usuários usando funções e políticas.

- **Funções:** um tipo de mecanismo de autorização de granulação grosseira que define permissões relacionadas às responsabilidades do usuário. Esse mecanismo fornece apenas um número limitado de funções de nível de serviço para autorização. Ao usar funções para conceder permissões, você também precisa atribuir outras funções das quais as permissões dependem, para que as permissões entrem em vigor. No entanto, as funções não são ideais para autorização refinada e controle de acesso seguro.
- **Políticas:** um tipo de mecanismo de autorização refinado que define as permissões necessárias para executar operações em recursos de nuvem específicos sob certas condições. Esse mecanismo permite uma autorização baseada em políticas mais flexível e atende aos requisitos de controle de acesso seguro. Por exemplo, você pode conceder aos usuários do DNS somente as permissões para gerenciar um determinado tipo de recursos do DNS. A maioria das políticas define permissões com base nas APIs. Para as ações de API suportadas pelo serviço do DNS, consulte [Políticas de permissões e ações suportadas](#).

Tabela 10-1 lista todas as funções ou políticas definidas pelo sistema suportadas pelo DNS.

Tabela 10-1 Funções ou políticas do DNS

Nome da função/política	Descrição	Tipo	Dependência
DNS FullAccess	Todas as permissões para o DNS.	Política definida pelo sistema	Nenhuma
DNS ReadOnlyAccess	Permissões de somente leitura para o DNS. Os usuários concedidos com essas permissões só podem exibir recursos do DNS.	Política definida pelo sistema	Nenhuma
DNS Administrator	Todas as permissões para o DNS.	Função definida pelo sistema	Essa função depende das funções Tenant Guest e VPC Administrator no mesmo projeto.

Tabela 10-2 lista as operações comuns suportadas por cada política ou função do sistema do DNS. Escolha as políticas de sistema apropriadas de acordo com esta tabela.

Tabela 10-2 Operações comuns suportadas por cada política ou função do DNS definida pelo sistema

Operação	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
Criação de uma zona pública	√	X	√

Operação	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
Visualização de uma zona pública	√	√	√
Modificação de uma zona pública	√	X	√
Exclusão de uma zona pública	√	X	√
Exclusão de zonas públicas em lotes	√	X	√
Desabilitação ou habilitação de uma zona pública	√	X	√
Criação de uma zona privada	√	X	√
Visualização de uma zona privada	√	√	√
Modificação de uma zona privada	√	X	√
Exclusão de uma zona privada	√	X	√
Exclusão de zonas privadas em lotes	√	X	√
Associação de uma VPC a uma zona privada	√	X	√
Desassociação de uma VPC de uma zona privada	√	X	√
Adição de um conjunto de registros	√	X	√
Visualização de um conjunto de registros	√	√	√
Modificar um conjunto de registros	√	X	√
Exclusão de um conjunto de registros	√	X	√
Excluir conjuntos de registros em lotes	√	X	√
Desabilitação ou habilitação de um conjunto de registros	√	X	√
Exportação de conjuntos de registros em lotes	√	X	√

Operação	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
Importação de conjuntos de registros em lotes	√	X	√
Criação de um registro de PTR	√	X	√
Visualização de um registro de PTR	√	√	√
Modificação de um registro de PTR	√	X	√
Exclusão de um registro de PTR	√	X	√
Exclusão de registros de PTR em lotes	√	X	√

Links úteis

- [O que é o IAM?](#)
- [Criação de um usuário e concessão de permissões do DNS](#)
- [Políticas de permissões e ações suportadas](#)

11 Integração com outros serviços

Figura 11-1 mostra as relações entre o DNS e outros serviços.

Figura 11-1 Serviços relacionados

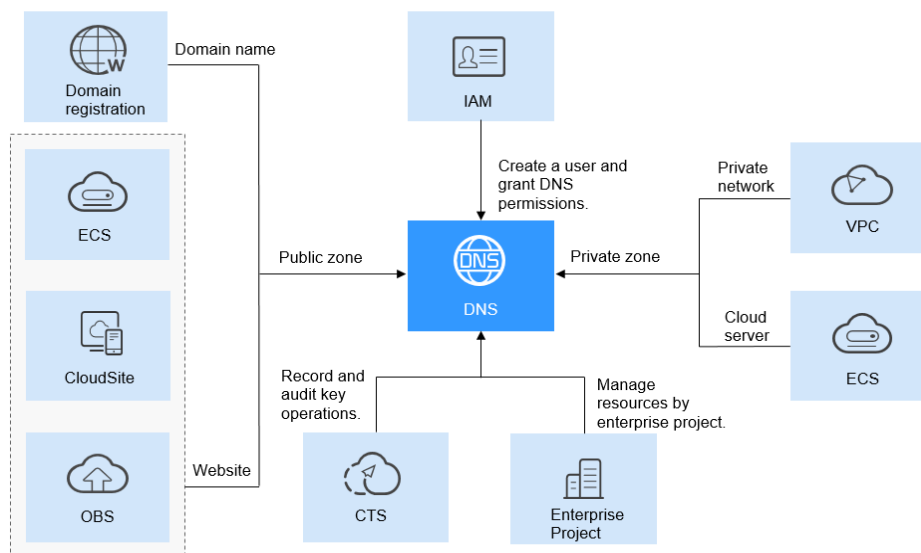


Tabela 11-1 mostra as relações entre o DNS e outros serviços.

Tabela 11-1 O DNS e outros serviços

Serviço relacionado	Descrição	Referência
Elastic Cloud Server (ECS)	Fornecer serviços de resolução de nomes de domínio público para ECSs.	Roteamento de tráfego da internet para um site
Virtual Private Cloud (VPC)	Cria VPCs para o serviço do DNS.	Roteamento de tráfego dentro das VPCs

Serviço relacionado	Descrição	Referência
Object Storage Service (OBS)	Hospeda recursos de sites estáticos para mapear nomes de domínio para intervalos.	Hospedagem de um site estático
Cloud Trace Service (CTS)	Registra as operações realizadas no serviço do DNS	Operações do DNS gravadas pelo CTS

12 Conceitos de produto

12.1 Formato de nome de domínio e hierarquia do DNS

Um nome de domínio válido atende aos seguintes requisitos:

- Um nome de domínio é segmentado usando períodos (.) em vários rótulos.
- Um rótulo de nome de domínio pode conter caracteres especificados em diferentes idiomas, letras, dígitos e hífen (-) e não pode começar ou terminar com um hífen.
- Um rótulo não pode exceder 63 caracteres.
- O comprimento total de um nome de domínio, incluindo o ponto final, não pode exceder 254 caracteres.

Um nome de domínio é dividido nos seguintes níveis com base em sua estrutura:

- Domínio raiz: . (um ponto)
- Domínio de nível superior: por exemplo, .com, .net, .org e .cn
- Domínio de segundo nível: subdomínios dos nomes de domínio de nível superior, como exemplo.com, exemplo.net e exemplo.org
- Domínio de terceiro nível: subdomínios dos nomes de domínio de segundo nível, como abc.example.com, abc.example.net e abc.example.org
- Os nomes de domínio de nível seguinte são expandidos da mesma forma adicionando prefixos aos nomes de domínio de nível anterior, como def.abc.example.com, def.abc.example.net e def.abc.example.org.

12.2 Conjunto de registros

Visão geral

Um conjunto de registros é uma coleção de registros de recursos que pertencem ao mesmo nome de domínio. Um conjunto de registros define tipos e valores de registros do DNS.

Se você tiver criado uma zona no console do DNS, poderá criar conjuntos de registros para expandir o nome de domínio ou registrar suas informações detalhadas.

Tabela 12-1 descreve os tipos de conjuntos de registros e seus cenários de aplicação.

Tabela 12-1 Usos do conjunto de registros

Tipo	Onde usar	Uso
A	Zonas públicas e privadas	Mapeia domínios para endereços IPv4.
CNAME	Zonas públicas e privadas	Mapeia um nome de domínio para outro ou vários nomes de domínio para um nome de domínio.
MX	Zonas públicas e privadas	Mapeia nomes de domínio para servidores de e-mail.
AAAA	Zonas públicas e privadas	Mapeia nomes de domínio para endereços IPv6.
TXT	Zonas públicas e privadas	Cria registros de texto para nomes de domínio. Os conjuntos de registros de TXT geralmente são usados nos seguintes cenários: <ul style="list-style-type: none"> ● Para registrar chaves públicas de DKIM para evitar fraudes por e-mail. ● Para registrar a identidade dos proprietários de nomes de domínio para facilitar a recuperação de nomes de domínio.
SRV	Zonas públicas e privadas	Servidores de registros que prestam serviços específicos.
NS	Zonas públicas e privadas	Delega subdomínios a outros servidores de nomes. <ul style="list-style-type: none"> ● Para zonas públicas, um conjunto de registros de NS é criado automaticamente e você pode adicionar conjuntos de registros de NS para subdomínios. ● Para zonas privadas, um conjunto de registros de NS é criado automaticamente e você não pode adicionar outros conjuntos de registros de NS.
SOA	Zonas públicas e privadas	Especifica o servidor do DNS autoritativo mestre para um nome de domínio. O conjunto de registros de SOA é criado pelo sistema e não pode ser adicionado manualmente.
CAA	Zona pública	Concede permissões de emissão de certificados para CAs. Os conjuntos de registros de CAA podem impedir a emissão de certificados HTTPS não autorizados.
PTR	Zona privada	Mapeia endereços IP para nomes de domínio.

Uso

Os conjuntos de registros são usados nos seguintes cenários:

- Encaminhar o tráfego da Internet para um site

Os conjuntos de registros de A e AAAA geralmente são usados para mapear nomes de domínio usados por sites para endereços IPv4 ou IPv6 de servidores da Web onde os sites são implantados.

Figura 12-1 Acessar um site pela Internet usando o nome de domínio



- Resolução de nome de domínio privado

Em uma rede privada, os conjuntos de registros de A e AAAA traduzem nomes de domínio privados em endereços IP privados.

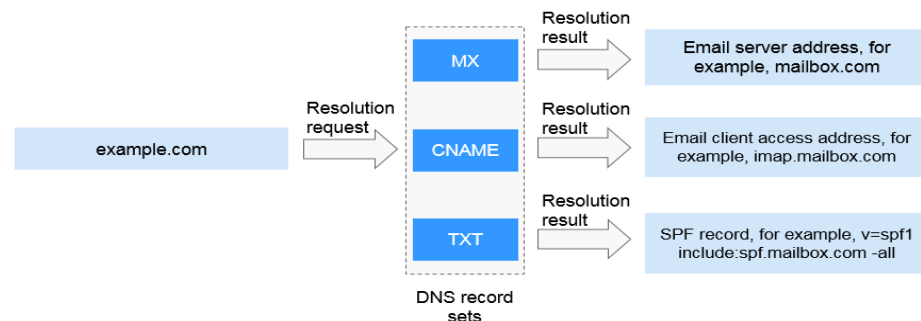
Figura 12-2 Resolução de nome de domínio privado



- Resolução de nome de domínio de e-mail

Os conjuntos de registros de MX, CNAME e TXT geralmente são usados para serviços de e-mail.

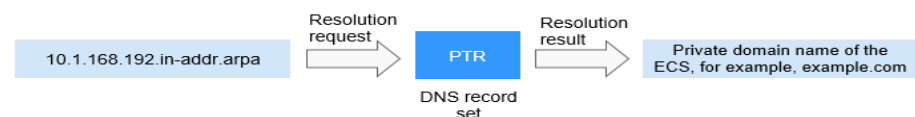
Figura 12-3 Resolução de nome de domínio de e-mail



- Resolução reversa em uma rede privada

Os registros de PTR traduzem endereços IP privados em nomes de domínio privados.

Figura 12-4 Resolução reversa em uma rede privada



Links úteis

Para obter detalhes sobre como adicionar e gerenciar conjuntos de registros, consulte [Conjunto de registros](#).

12.3 Região e AZ

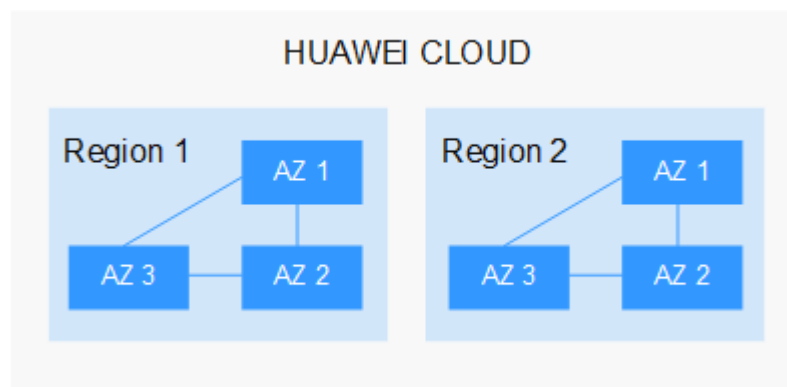
Conceito

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 12-5 mostra a relação entre regiões e AZs.

Figura 12-5 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](#).

12.4 Projeto

Os projetos são usados para agrupar e isolar recursos de nuvem, incluindo recursos de computação, armazenamento e rede. Vários projetos podem ser criados para uma conta. Um projeto pode ser um departamento ou uma equipe de projeto.

As zonas públicas são recursos de nível global, enquanto as zonas privadas e os registros de PTR são recursos de nível regional. Zonas privadas e registros de PTR são isolados e gerenciados com base em projetos. Você precisa criar, consultar e configurar zonas privadas ou registros de PTR em regiões e projetos específicos.

13 Histórico de alterações

Lançado em	Descrição
30/10/2021	Esta edição é a sétimo lançamento oficial, que incorpora as seguintes alterações: Adição das seguintes seções: Gerenciamento de permissões
12/02/2020	Esta edição é o sexto lançamento oficial, que incorpora as seguintes alterações: Adição das seguintes seções: Funções Otimização das seguintes seções: <ul style="list-style-type: none">● Resolução de nome de domínio público● Resolução de nome de domínio privado● Conjunto de registros
02/07/2019	Esta edição é a quinta versão oficial, que incorpora as seguintes alterações: Adição da descrição para linhas de ISP e região em Resolução inteligente .
25/06/2019	Esta edição é a quarta versão oficial, que incorpora as seguintes alterações: Adição da descrição para regiões e AZs em Região e AZ .
05/03/2019	Esta edição é a terceira versão oficial, que incorpora as seguintes alterações: Adição de links em Integração com outros serviços .
20/01/2019	Esta edição é a segunda versão oficial, que incorpora as seguintes alterações: Adição do processo de resolução de nomes de domínio e cenários de aplicação.
22/11/2018	Esta edição é o primeiro lançamento oficial.