

Domain Name Service

Service Overview

Issue 01
Date 2026-01-23



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

| | |
|--|-----------|
| 1 What Is DNS? | 1 |
| 2 Product Concepts | 3 |
| 3 Functions | 12 |
| 3.1 Public DNS Resolution | 12 |
| 3.2 Private DNS Resolution | 14 |
| 3.3 Reverse Resolution | 19 |
| 3.4 Hybrid Cloud Resolution | 21 |
| 4 Constraints | 24 |
| 5 Permissions | 27 |
| 6 Integration with Other Services | 33 |
| 7 Security | 35 |
| 7.1 Shared Responsibilities | 35 |
| 7.2 Identity and Access Control | 37 |
| 7.3 Auditing and Logging | 37 |
| 7.4 Resilience | 37 |
| 7.5 Monitoring Security Risks | 38 |
| 7.6 Certificates | 38 |

1 What Is DNS?

Domain Name Service (DNS) is a highly available and scalable authoritative Domain Name System (DNS) web service that translates domain names (such as `www.example.com`) into IP addresses (such as `192.1.2.3`) required for network connection. The DNS service allows end users to visit your websites or web applications using domain names.

The DNS service is free and is enabled by default.

Basic Functions

The DNS service provides the following functions:

- **Public DNS resolution**
Maps domain names to public IP addresses so that end users can access your website or web applications over the Internet.
- **Private DNS resolution**
Translates private domain names into private IP addresses to facilitate access to cloud resources within VPCs.
- **Reverse resolution**
Obtains a domain name based on an IP address. Reverse resolution, or reverse DNS lookup, is typically used to affirm the credibility of email servers.
- **Hybrid cloud resolution**
A DNS resolver allows on-premises data centers to access the DNS on the cloud or cloud servers to access on-premises service domain names, as well as deploys IP addresses in the network segment `100.x.x.x` of the DNS service in the customer's VPC to prevent network segment conflicts on the hybrid cloud.

Advantages

The DNS service has the following advantages:

- High performance
A single DNS node can handle tens of millions of concurrent queries, allowing end users to access your website or application much faster.
- Easy access to cloud resources

Your ECSs can communicate with each other and with other resources within VPCs using private domain names. Traffic is kept within your internal network, which reduces network latency and improves security.

For more details, see [Configuring Private Domain Names for ECSs](#).

- Smooth service migration

You can transfer the record sets configured for an in-use website domain to the Huawei Cloud DNS service. You can create a public zone and add record sets on the DNS console before the migration. In this way, your website services are not interrupted during the migration.

- Isolation of core data

A private DNS server provides domain name resolution for ECSs carrying core data, enabling secure, controlled access to such data. You do not need to bind EIPs to these ECSs.

Accessing the DNS Service

The cloud platform provides a web-based management console as well as REST APIs through which you can access the DNS service.

- Management console

A web-based management console is provided for you to perform operations on the DNS service.

- If you have registered an account, log in to the [DNS console](#).
- If you do not have an account, create one by following the instructions in [Before You Start](#).

With a few steps, you can start using the DNS service for domain name resolution.

- APIs

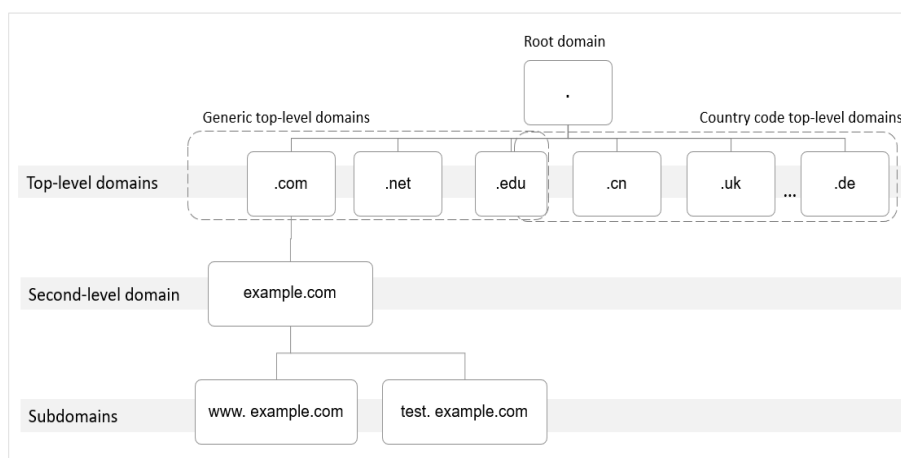
REST APIs are provided for accessing the DNS service. You can also use the provided APIs to integrate DNS into a third-party system for secondary development. For details, see the [Domain Name Service API Reference](#).

2 Product Concepts

Domain Name Hierarchy

The domain name resolution involves a hierarchical structure and often uses recursive queries.

The following uses example.com as an example to describe the structure and levels of a domain name.



- **Root domain**

A period (.) is the designation for the root domain.

A fully qualified domain name (FQDN) ends with a period (example.com.). When you enter a domain name (example.com) in the browser, the DNS system will automatically add a period in the end.

Root domain names are resolved by root name servers that hold the addresses of top-level domain servers.

- **Top-level domain**

Below the root domain are top-level domains, which are categorized into two types:

- Generic top-level domain (gTLD), such as .com, .net, .org, and .top
- Country code top-level domain (ccTLD), such as .cn, .uk, and .de

Top-level domains are resolved by top-level domain servers that hold the addresses of second-level DNS servers. For example, the top-level domain server of .com saves the addresses of all DNS servers of second-level domains that end with .com.

- **Second-level domain**

Second-level domains (such as example.com) are subdomains of top-level domains and are resolved by second-level DNS servers, which provide authoritative domain name resolution services.

For example, if you purchase example.com from a domain name registrar and set a DNS server for the domain name, the DNS server will provide authoritative resolution for example.com, and its address will be recorded by all top-level domain servers.

If you host domain names on the Huawei Cloud DNS service, authoritative DNS servers will provide authoritative resolution services for your domain names.

- **Subdomain**

Second-level domains can be further divided into subdomains (such as www.example.com) to indicate specific servers or services.

DNS Hierarchy

DNS also operates through a hierarchical structure. At the top is the root name server, followed by top-level domain servers, authoritative servers, local DNS and cache servers. Each level plays a specific role in the resolution process and works together for domain name resolution. This structure ensures efficient, reliable, and scalable domain name resolution.

- **Root name server (Root server)**

Root name servers are at the top of the DNS hierarchy and direct queries for records to an appropriate top-level domain server. When a local DNS server does not have the IP address cached for a domain name, it will query a root name server, aiming to obtain the IP address.

- **Top-level domain (TLD) server (TLD server)**

TLD servers handle queries related to specific generic top-level domains such as .com, .org, and .net, and country code top-level domains, such as .cn and .us.

Each top-level domain has its own set of servers that manage the DNS entries for domains within that top-level domain. For example, when a client wants to access www.example.com, the local DNS server sends the request to the top-level domain server of .com. Then, the top-level domain server of .com returns the address of the authoritative DNS server of the second-level domain example.com.

- **Authoritative server (NS server)**

Authoritative DNS servers are the final word on the mapping between specific domain names and their associated IP addresses. For example, the authoritative DNS server of example.com will return the IP address mapped to the subdomain www.example.com.

- **Local DNS server (Local DNS)**

Local DNS servers are the DNS servers that user devices (like phones and computers) utilize to connect to the internet. They are often provided by

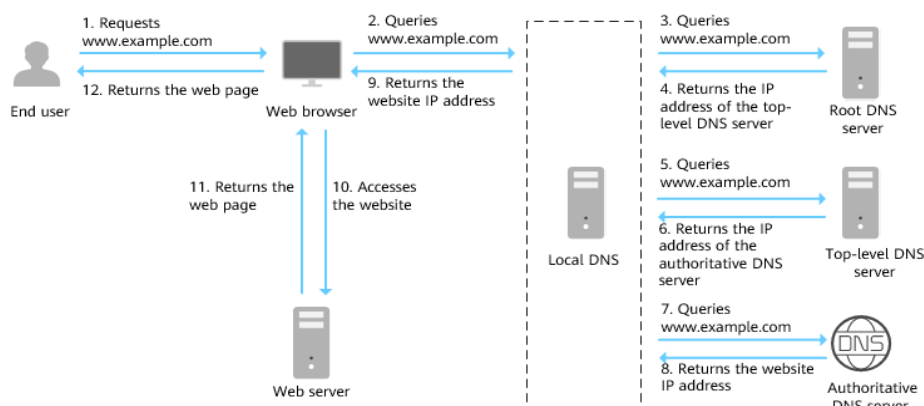
Internet Service Providers (ISPs) or organizations handle recursive DNS requests from clients. When a user requests a domain name, the local DNS server initiates a recursive query to find the corresponding IP address. It searches layer by layer through the DNS hierarchy until it finds the authoritative server that holds the correct IP address. Once found, the local server caches this information to speed up future requests for the same domain.

You can also choose a public DNS server, for example, 114.114.114.114 and 8.8.8.8, as your local DNS server.

DNS Resolution Process

Figure 2-1 shows the process for accessing a website using the domain name `www.example.com`.

Figure 2-1 Domain name resolution



1. An end user enters **www.example.com** in the address box of a browser.
2. The query for `www.example.com` is routed to the local DNS server.
Local DNS servers are usually provided by the Internet service provider to cache domain name information and perform recursive lookup.
3. If the local DNS server does not find any records in the cache, it routes the request for `www.example.com` to the root name server.
4. The root name server returns the address of the top-level domain server of `.com` to the local DNS server.
5. The local DNS server sends the request to the top-level domain server of `.com`.
6. The top-level domain server of `.com` returns the address of the authoritative DNS server which provides authoritative records for `example.com`.
7. The local DNS server sends the request to the authoritative DNS server of `example.com`.

If you have hosted `www.example.com` on the DNS service and configured [Huawei Cloud DNS name servers](#), these name servers will provide authoritative DNS for the domain name.

8. The authoritative DNS server returns the IP address mapped to `www.example.com` to the local DNS server.

9. The local DNS server returns the IP address to the web browser.
10. The web browser accesses the web server with the IP address.
11. The web server returns the web page to the browser.
12. The end user views the web page using the browser.

DNS Cache

DNS cache is temporary storage that stores DNS records of domain names. It is usually found on user devices, routers, and the servers of Internet Service Providers (ISPs). DNS cache improves network performance and efficiency.

When a user device accesses a domain name, the device first checks the local DNS cache. If the DNS record is found in the local DNS cache, the device uses it directly. If the information is not found there, the device then queries its DNS server provided by the ISP or other DNS servers and stores the queried data in the cache for future use.

Helpful Links

- [When Will a New Record Set Be Applied?](#)
- [When Will the Modification or Deletion of a Record Set Be Applied?](#)

TTL

Time-to-live (TTL) specifies how long a local DNS server can cache record sets. A proper TTL value helps balance DNS server load and resolution speed, while also affecting how quickly DNS changes are applied.

When receiving requests for a domain name, the local DNS server asks the authoritative DNS server for the required DNS record, and then caches the record for a period of time. During this period, if the local DNS server receives requests for this domain name again, it will not request the record from the authoritative DNS server, but directly returns the cached record.

The time records are cached on the local DNS server is specified by the TTL value. You can set it when adding record sets in public or private zones. For details, see [Managing Record Sets](#).

The effective time of the following operations depends on the TTL value (to accelerate the process, decrease the TTL value):

- [When Will a New Record Set Be Applied?](#)
- [When Will the Modification or Deletion of a Record Set Be Applied?](#)
- [When Will New DNS Server Addresses Be Applied?](#)

Recursive Query/Recursive Resolution

Recursive query and recursive resolution are fundamental concepts in DNS resolution. A recursive query is initiated by a client to a DNS resolver, and that resolver is responsible for performing the recursive resolution and ultimately returning the DNS results to the client.

- **Recursive query:** a type of DNS queries sent from a client (such as a user's computer) to a DNS resolver. A client sends requests to a DNS resolver, and

the resolver takes full responsibility for the entire resolution process until it finds the final answer and returns it to the client. In a recursive query, the client only sends the request to the first DNS server.

- **Recursive resolution:** a method used by a DNS resolver to process recursive queries. When receiving a recursive query, the DNS resolver will work down the hierarchy, starting from the root servers, then to top-level domain servers, and finally to the authoritative servers for the query result. Finally, the DNS resolver will return the query result to the client. Users do not need to handle complex query processes.

Helpful Links

[Configuring Recursive Resolution for Subdomains](#)

DNSSEC

Domain Name System Security Extensions (DNSSEC) provides digital signatures and public key cryptography to ensure the integrity and authenticity of DNS response packets and to defend against common attacks such as DNS spoofing and cache pollution. This prevents you from being redirected to unexpected addresses and protects your core services.

Working principles and main functions

- **Digital signatures for data integrity:** Digital signatures are added to DNS records so that data integrity can be verified. This ensures that DNS records are not tampered with.
- **Public key cryptography for trusted data sources:** Public keys are used to verify signatures for establishing trust in data sources.
- **A full chain of trust to prevent DNS spoofing and cache pollution:** A full chain of trust is formed from the root DNS servers to the top-level domain servers and then to the authoritative DNS servers. This prevents attackers from inserting false records into the DNS cache.

Helpful Links

[Configuring DNSSEC](#)

DKIM

DomainKeys Identified Mail (DKIM) is a technical standard used to verify the authenticity and integrity of email sources. It uses digital signatures to prevent email spoofing and tampering.

Key principles and working process

1. **Key generation and distribution**
 - a. DKIM uses a private/public key pair.
 - b. The private key is kept on the sender's email server and is used to sign emails.
 - c. The public key is added to the DNS records for the sending domain and is usually used as a TXT record for the receiver to query.
2. **Email signature process**

- a. The sending email server uses the private key to generate a digital signature for the specific part of the email (such as the header and body).
 - b. DKIM signatures are embedded within the **DKIM-Signature** header field, including a cryptographic hash of the email content, the algorithm used for signing (like RSA-SHA256), and the sending domain.
3. **Verification by the recipient**
- a. The receiving server parses the **DKIM-Signature** header field of the email to extract the signature information.
 - b. The receiving server looks up the DNS records for the sending domain and retrieves the public key for the sending domain.
 - c. The public key decrypts the encrypted hash sent. The receiving server computes its own hash and compares it with the one received in the message.
 - d. If the two match, the message is let through, meaning that the mail has not been tampered with and its source is authentic. Otherwise, the email may be flagged as spam or rejected.

Example:

Here is what a typical DKIM-Signature header field looks like:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=example.com;
s=mail; h=From:Subject:Date:Message-ID:To:MIME-Version:Content-Type;
bh=abc123==; b=def456==;
```

- **v=1**: Specifies the DKIM version.
- **a=rsa-sha256**: Indicates the algorithm used for signing the messages.
- **c=relaxed/relaxed**: Sets the canonicalization posture for the sending domain.
- **d=example.com**: Specifies the sending domain.
- **s=mail**: Indicates the selector of the DKIM key.
- **h=...**: Lists the header fields that were included in the signature.
- **bh=...**: Represents the hash of the email body.
- **b=...**: Contains the digital signature itself.

SPF

Sender Policy Framework (SPF) is a technique designed to authenticate email senders to prevent email spam and phishing attacks. It enables the receiving mail server to check whether an incoming email comes from a domain authorized by that domain's administrators, thereby verifying the legitimacy of the email.

Key principles and working process

1. **IP address authorization**

The domain owner configures a TXT or SPF record in DNS that lists all authorized sending IP addresses or servers.

2. **Verification process**

- a. When the email server receives an email, it checks the Return-Path (sender address) of the email.
- b. The email server queries the SPF record of the sender's domain name through DNS.

- c. This SPF record is used to check whether the IP address from which an email is sent is authorized.
- d. When the verification succeeds, the mail is legitimate. When the verification fails, the mail can be marked as spam or rejected.

Example:

The following is an example of an SPF TXT record.

```
v=spf1 include:spf.example.com -all
```

- **v=spf1**: Indicates that it is an SPF record and the version is 1.
- **include:spf.example.com**: Indicates that the SPF record contains the **spf.example.com** domain.
- **-all**: Specifies that any IP address not explicitly authorized in the record should be treated as a hard fail, meaning emails from them should be rejected. (~ indicates a soft fail qualifier while - indicates a hard fail qualifier.)

If ~**all** is specified here, it indicates a soft failure qualifier. Emails from any IP address not explicitly authorized in the record will be marked as potentially suspicious but will not be rejected.

Wildcard DNS Record Set

A wildcard record set with its name set to an asterisk (*) can map all subdomains of a domain name to the same IP address or other destination.

For example, a wildcard DNS record like ***.example.com** acts as a catch-all for subdomains. **www.example.com**, **abc.example.com**, and **test.example.com** can all be mapped to the same IP address or destination that ***.example.com** will be mapped to.

Scenarios:

- **Static resource hosting**
All subdomains can be mapped to the same CDN or static resource server. This improves resource loading speed and management efficiency.
- **Test and development environments**
You can quickly create and test multiple subdomains without frequently adjusting DNS settings. This facilitates development.
- **User-generated content platforms**
Users can create personal subdomain-based blogs or websites. All subdomains are automatically mapped to the same server. This ensures easier management.
- **API service**
Multiple subdomains can be mapped to the same API service where API requests are centrally managed for more flexible services.
- **Multilingual or multi-regional sites**
All subdomains are mapped to the same multilingual or multi-regional website where users can view content in different languages or regions. This optimizes user experience.
- **Temporary or dynamic subdomain**

You can quickly create temporary subdomains for promotions or events without manual configuration, improving the response speed.

Helpful Links

[Configuring a Wildcard DNS Record Set](#)

Domain Name Owner

A domain name is owned by the person or organization who registered it through a domain registrar. Details about a domain name owner are as follows:

- **Ownership and control:** Domain name owners have the right to use domain names as they see fit, for example, directing them to specific servers and creating subdomains.
- **Registration and maintenance:** Domain name owners must register their domain names with a registrar and pay annual renewal fees to maintain ownership and prevent expiration.
- **Information management:** Domain name owners are generally required to provide personal information, including their name, address, and email address, during the registration process. This information is stored in a publicly accessible database called the WHOIS database. However, privacy protection services can be used to hide their personal details.
- **Management permissions:** Domain name owners can manage DNS settings, control website resolution, implement security measures like DKIM and SPF records, and transfer domain names to other registrars.
- **Renewal and transfer:** Domain name owners should renew their domain registrations before the expiration date. Domain names can be transferred through registrars or traded in the secondary market.

DNS Service Provider

A DNS service provider manages the Domain Name System (DNS), which translates domain names into server IP addresses. A DNS service provider provides the following functions:

- **Domain name resolution:** translates domain names into IP addresses so that users can access target websites by entering a domain name.
- **DNS record management:** allows users to set and manage various DNS records, like A, CNAME, and MX records.
- **High availability and stability:** leverages multi-node distribution to ensure the DNS resolution stability and efficiency.
- **Value-added services:** provides functions such as load balancing, CDN integration, anti-DDoS, and intelligent resolution to improve website performance and security.

Project

A project is used to group and isolate resources, including compute, storage, and networking resources. A project can be a department or a project team.

Multiple projects can be created under one account.

Public zones are global resources, while private zones and PTR records are regional resources. Private zones and PTR records are isolated and managed based on projects. You need to create, query, and configure private zones or PTR records in specific regions and projects.

Region and AZ

For details, see [Region and AZ](#).

3 Functions

3.1 Public DNS Resolution

What Is Public DNS Resolution?

Public DNS resolution translates a domain name like `www.example.com` into an IP address like `1.2.3.4` for routing traffic over the Internet. It is implemented by public DNS servers, including authoritative and non-authoritative DNS servers. An authoritative DNS server stores various DNS records, including A, CNAME, and MX records, and returns accurate responses to DNS queries.

Authoritative DNS services are highly available and scalable authoritative DNS resolution services and domain name management services. They are typically provided by either domain name registrars or cloud service providers.

If you host your domain names on the Huawei Cloud DNS service, DNS will provide public domain name resolution for your website and email servers. Visitors can access your website, mailbox, or web application by entering the desired domain name in the address box of their browser.

Scenarios

- **Website building**

An A record set can map a website domain name to the numerical address of the server where your website is hosted. After an A record set is added for the domain name, users can access your website using the domain name.
- **Email**

An MX record set can map a domain name to the email server address provided by an email service provider. After an MX record set is added for the domain name, emails can be sent and received properly.
- **Heavy-traffic applications**

When a large website is deployed on multiple servers, you can configure weighted routing to distribute requests proportionally among servers. This helps balance server load.
- **Global traffic scheduling**

When visitors are from different carriers or geographical locations, you can configure ISP and region lines to return different resolution results based on the networks or geographical locations of visitors' IP addresses.

- **Service acceleration with CDN**

You can add a CNAME record to map a domain name to the alias domain provided by the CDN service provider. This speeds up website response or download.

Advantages

- **Deployment in 20+ countries/regions**

End users around the world can resolve domain names with low latency.

- **High performance**

Huawei's next-generation Data Plane Development Kit (DPDK) offers resolution acceleration services. This allows DNS to handle hundreds of millions of concurrent queries.

- **Robust security**

DNS defends services against various DDoS attacks with Huawei's powerful anti-DDoS devices and extensive experience in security protections.

- **Smooth switchover**

You can transfer the record sets configured for an in-use website domain to the Huawei Cloud DNS service. You can create a public zone and add record sets on the DNS console before the migration. In this way, your website services are not interrupted during the migration.

Functions

Table 3-1 Functions involved in public DNS resolution

| Function | Description |
|-------------------|---|
| Public zone | A public zone hosts the record sets for a domain name that is accessible on the public Internet. You can create, modify, delete, enable, disable, and view public zones. For details, see Overview . |
| Domain name level | DNS allows you to create public zones for second-level domain names and their subdomains. <ul style="list-style-type: none">• For domains with single-level suffixes such as .com, you can create zones like example.com and www.example.com.• For domains with two-level suffixes such as .com.cn, you can create zones like example.com.cn and www.example.com.cn. |

| Function | Description |
|--------------------------|--|
| Record set | A record set is a collection of resource records that belong to the same domain name. A record set defines the resolution type and value of a domain name. You can add, modify, delete, view, disable, or enable record sets of the A, CNAME, MX, AAAA, TXT, SRV, NS, and CAA types for public zones. For details, see Overview . |
| Reclaiming a public zone | If a public zone has been created for your domain name by another user, you can reclaim it by proving that you are the holder of the domain name. For details, see Reclaiming a Public Zone . |
| Wildcard DNS record set | For a second-level domain, you can add a record set with the record set name set to an asterisk (*), so traffic will be routed to all subdomains of that domain name. For details, see Configuring a Wildcard DNS Record Set . |
| TTL | Time-to-live (TTL) specifies how long a local DNS server can cache record sets before it must request fresh information from an authoritative server. It is measured in seconds. The TTL value ranges from 1 to 2147483647 . |
| Weight | The weight assigned to each record determines the proportion of DNS queries that will be routed to that record. If a domain name has multiple records with the same type and line, you can set different weights for each record. For details, see Configuring Weighted Routing . |
| Checking domain name | You can check whether the record sets of website or email domains have been applied. If any record set is not applied, you can fix the issue by following the provided suggestions. For details, see Checking a Domain Name . |
| Batch operations | You can add and transfer zones, and add, modify, and delete record sets in batches. |

Helpful Links

- For details about how to configure public DNS resolution for a website, see [Routing Internet Traffic to a Website](#).

3.2 Private DNS Resolution

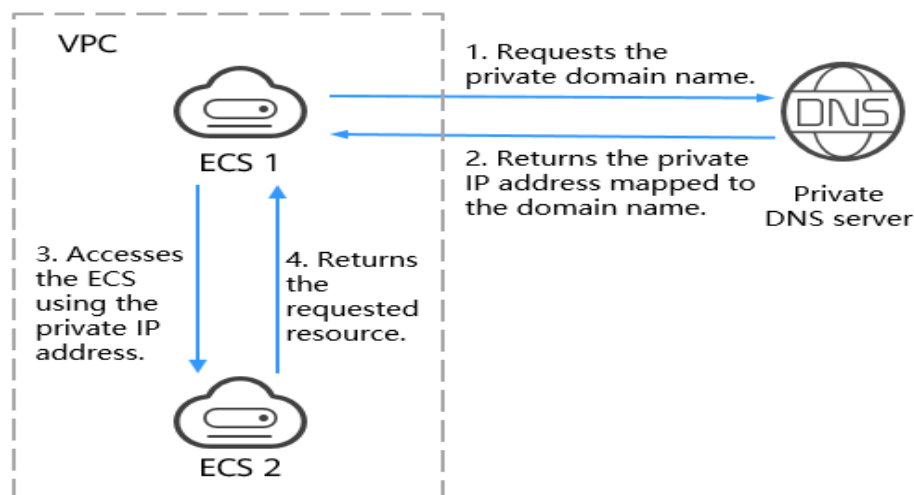
What Is Private DNS Resolution?

Private DNS resolution translates domain names like `ecs.com` and their subdomains used within one or more VPCs to private IP addresses (such as `192.168.1.1`). With private DNS resolution, ECSs within a VPC can communicate

with each other using private domain names and access cloud services, such as OBS and SMN, over a private network.

Figure 3-1 shows how a private domain name is resolved by a private DNS server.

Figure 3-1 Process for resolving a private domain name



When an ECS in the VPC requests to access a private domain name, the private DNS server directly returns a private IP address mapped to the domain name.

Private zones allow you to:

- Create custom private domain names in your VPCs.
- Associate one or more VPCs with a private zone.
- Use private domain names to access ECSs as well as OBS and SMN resources in the VPCs more quickly, preventing DNS spoofing.

Scenarios

Private zones are applicable to the following scenarios:

Managing ECS Hostnames

You can plan hostnames based on the locations, usages, and account information of ECSs, and map the hostnames to private IP addresses, helping you manage ECSs more easily.

For example, if you have deployed 20 ECSs in an AZ, 10 for website A and 10 for website B, you can plan their hostnames (private domain names) as follows:

- ECSs for website A: weba01.region1.az1.com – weba10.region1.az1.com
- ECSs for website B: webb01.region1.az1.com – webb10.region1.az1.com

After you configure the hostnames, you will be able to quickly determine the locations and usages of ECSs during routine management and maintenance.

For details, see [Configuring Private Domain Name Resolution for ECSs](#).

Keeping Your Website Up and Running Even While Your Server Is Being Replaced

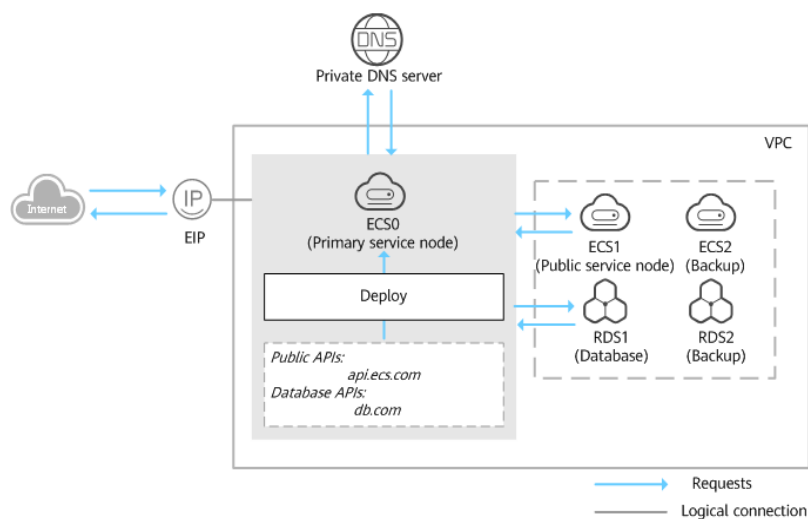
As the number of Internet users is continuously increasing, a website or web application deployed on a single server can hardly handle concurrent requests during peak hours. A common practice is to deploy the website or application on multiple servers and distribute the load across the servers.

These servers are in the same VPC and communicate with each other using private IP addresses that are coded into internal APIs called among the servers. If one of these servers is replaced, its private IP address changes. As a result, you need to change this IP address in the APIs and re-publish the website. This poses challenges for system maintenance.

If you create a private zone for each server and configure record sets to map their private domain names to the private IP addresses, they will be able to communicate using private domain names. When you replace any of the servers, you only need to change the private IP address in the record set, instead of modifying the code.

Figure 3-2 illustrates such use of private domain name resolution.

Figure 3-2 Configuring private DNS for cloud servers



The ECSs and RDS instances are in the same VPC.

- ECS0: primary service node
- ECS1: public service node
- RDS1: service database
- ECS2 and RDS2: backup service node and backup database

When ECS1 becomes faulty, ECS2 must take over. However, if no private zones are configured for the two ECSs, you need to change the private IP addresses in the code for ECS0. This will interrupt services, and you will need to publish the website again.

Now assume that you have configured private zones for the ECSs and have included their private names in the code. If ECS1 becomes faulty, you only need to

change the DNS records to direct traffic to ECS2. Services are not interrupted, and you do not need to publish the website again.

For more details, see [Configuring a Private Domain Name for an ECS](#).

Accessing Cloud Resources

The comparison between private DNS and public DNS servers is as follows:

- If a public DNS server is configured for subnets of the VPC associated with a private zone, domain name requests to access cloud resources from ECSs in the VPC will be directed to the Internet.

The ECSs access Huawei cloud services such as OBS and SMN over the Internet. This increases the network latency and reduces access speed.

Steps 1 to 10 on the right of [Figure 3-3](#) show the resolution process.

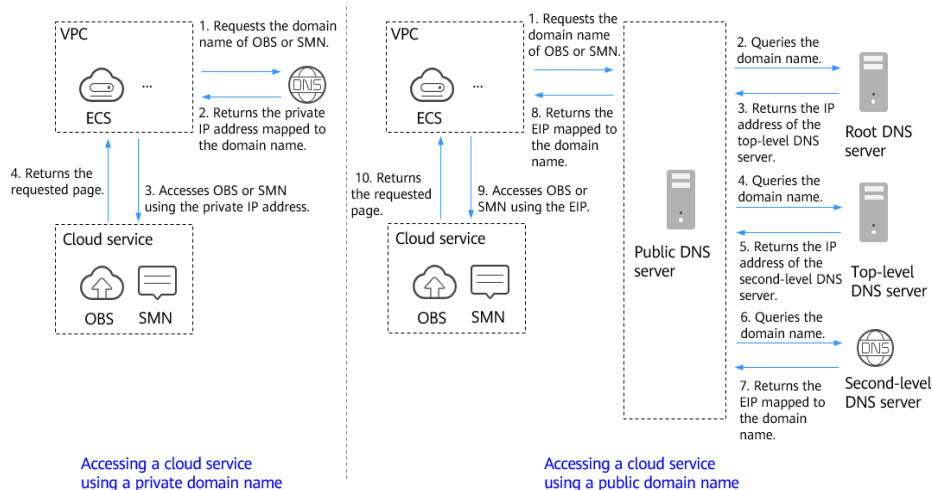
- If a Huawei Cloud private DNS server is configured for the subnet, the private DNS server directly processes the requests to access cloud services.

When the ECS accesses the Huawei cloud services, the private DNS server returns their private IP addresses, instead of routing requests over the Internet. This reduces network latency and improves access speed.

Steps 1 to 4 on the left of [Figure 3-3](#) show the resolution process.

To make your ECS accessible within the private network, change the default DNS servers of the ECS to private DNS servers. For details, see [How Do I Change Default DNS Servers of an ECS to Huawei Cloud Private DNS Servers?](#)

Figure 3-3 Accessing cloud services



Advantages

- **Easy access to cloud resources**

Your ECSs can communicate with each other and with other resources within VPCs using private domain names. Traffic is kept within your internal network, which reduces network latency and improves security.

For more details, see [Configuring a Private Domain Name for an ECS](#).

- **Isolation of core data**

A private DNS server provides domain name resolution for ECSs carrying core data, enabling secure, controlled access to such data. You do not need to bind EIPs to these ECSs.

Functions

Table 3-2 Private zone operations

| Function | Description |
|---|--|
| Private zone | <p>A private zone hosts a private domain name and record sets for this domain name for domain name resolution. It is applied only to its associated VPCs. DNS allows you to create, modify, delete, and view private zones, associate private zones with VPCs, and disassociate private zones from VPCs.</p> <ul style="list-style-type: none">• Private zones can be created without registration.• Each private zone must be unique in an associated VPC. <p>For details, see Overview.</p> |
| Associating a private zone with or disassociating a private zone from a VPC | <p>You can associate a private zone with a VPC or disassociate a private zone from a VPC.</p> <p>For details, see Associating a VPC with a Private Zone and Disassociating a VPC from a Private Zone.</p> |
| Record set | <p>A record set is a collection of resource records that belong to the same domain name. A record set defines the resolution type and value of a domain name. You can add, modify, delete, or view A, CNAME, MX, AAAA, TXT, PTR, and SRV record sets for private zones.</p> <p>For details, see Overview.</p> |
| Wildcard DNS record set | <p>You can add record sets for all subdomains of a private domain name. DNS provides resolution services for all subdomains.</p> <p>For details, see Configuring a Wildcard DNS Record Set.</p> |
| TTL | <p>Time-to-live (TTL) specifies how long a local DNS server can cache record sets. It is measured in seconds. The TTL value ranges from 1 to 2147483647.</p> |

Helpful Links

[Configuring Private Domain Name Resolution for ECSs](#)

3.3 Reverse Resolution

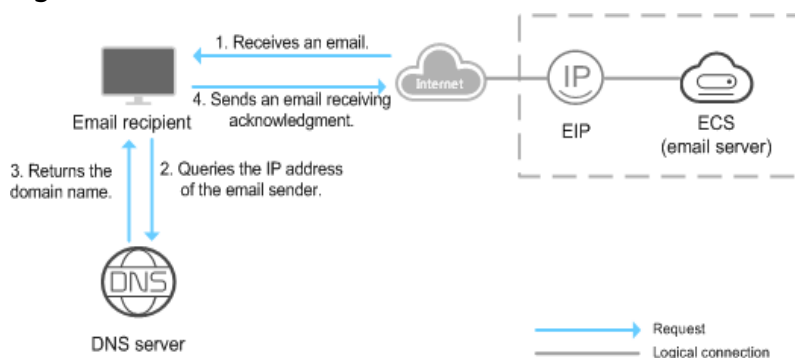
What Is Reverse Resolution?

A PTR record provides the domain name associated with an IP address. It is the opposite of a regular DNS lookup. PTR records are used to verify the mapping between IP addresses and domain names. PTR records are used in many network applications. For example, email servers use reverse resolution to verify the sender's IP address to reduce spam and network fraud.

After a recipient server receives an email, it checks whether the IP address and domain name of the sender server are trustworthy and determines whether the email is spam. If the recipient server fails to obtain the domain name mapped to the sender's IP address, it concludes that the email is sent by a malicious host and rejects it. It is necessary to configure pointer records (PTR) to point the IP addresses of your email servers to domain names.

In the following figure, an ECS serves as an email server, and a PTR record is configured to map the EIP of the ECS to the domain name configured for accessing the email server.

Figure 3-4 Reverse resolution



For example, enterprise A deploys their email service on an ECS (email server) and binds an EIP to the ECS to enable public network communication. Enterprise B receives emails from a local email recipient (such as an enterprise email client or server) and uses DNS for reverse lookup verification.

1. **Enterprise A sends an email, and enterprise B receives the request:** The email recipient (for example, the local email server) receives an email from the external network.
2. **Enterprise B triggers reverse resolution to query the domain name mapped to the email server IP address of enterprise A:** To verify that the email is not a spam email from a forged IP address, the email recipient of enterprise B proactively sends a reverse resolution request to the DNS server to query the domain name mapped to the email server IP address of enterprise A (that is, the EIP).
3. **The DNS server returns the resolution result:** The DNS server returns the domain name (for example, mail.companyA.com) mapped to the email server IP addresses of enterprise A to the email recipient of enterprise B based on the mapping between the IP address and domain name.

4. **If the verification is successful, the recipient receives the email:** The email recipient of enterprise B checks whether the domain name obtained from the reverse resolution is the same as the actual domain name of the email. If the domain names are the same, the email recipient returns a message indicating that the email has been received to the EIP (associated with the ECS) of enterprise A.

NOTE

The preceding describes the reverse resolution process of the DNS service. Information about how the email recipient checks the credibility of the sender's IP address and whether the domain name is available on the Internet is not provided here.

If no PTR records are configured, the recipient server will treat emails from the email server as spam or malicious and discard them.

Scenarios

Reverse resolution is mainly used for email server verification in the following scenarios:

- **Anti-spam:** Email servers usually use reverse resolution to verify the sender's IP address. If the IP address cannot be resolved to a valid domain name or the resolution result does not match the sender information in the email, the email may be marked as spam or rejected.
- **SPF record verification:** An SPF record specifies the IP addresses authorized to send emails from a domain name. Reverse resolution checks whether the sender's IP address is in the SPF record.

Advantages

- **Improved email delivery rate**
You can configure correct reverse DNS records to improve the email delivery rate and reduce the risk of being identified as spam.
- **Enhanced network security**
Reverse resolution helps network administrators quickly locate and identify devices on the network and respond to and handle security events. For example, when a DDoS attack occurs, you can use reverse resolution to quickly locate the attack source.
- **Simplified troubleshooting**
Reverse resolution can translate an IP address into a domain name that is easier to understand. This helps technical personnel quickly locate faults.

Functions

Table 3-3 Common functions of reverse resolution

| Function | Description |
|------------|--|
| PTR record | DNS allows you to configure PTR records for EIPs. You can create, modify, delete, and view PTR records. For details, see Overview . |

| Function | Description |
|----------|--|
| TTL | Time-to-live (TTL) specifies how long a local DNS server can cache record sets. It is measured in seconds. The TTL value ranges from 1 to 2147483647 . |

Helpful Links

For details about how to configure a PTR record for an email server, see [Configuring a PTR Record for an Email Server](#).

3.4 Hybrid Cloud Resolution

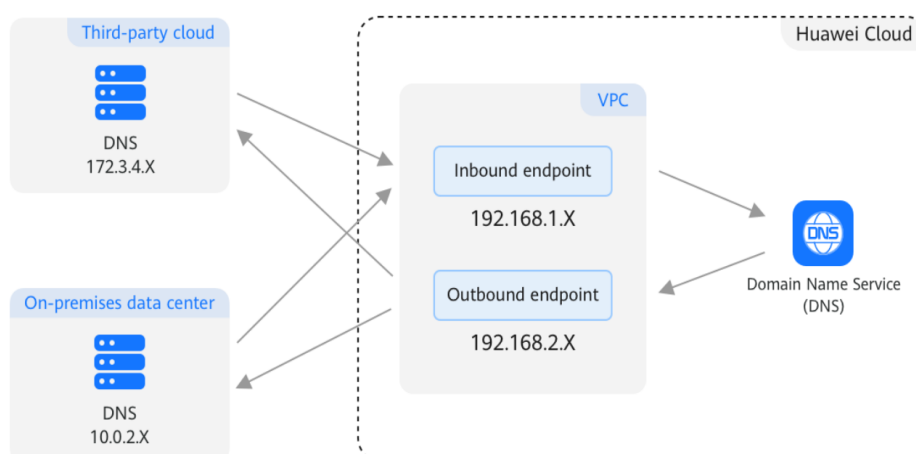
What is hybrid cloud resolution?

DNS Resolver answers DNS queries to and from your on-premises data center after your data center is connected to the cloud over Direct Connect or VPN.

Generally, on-premises data centers can access cloud resources over a Direct Connect or VPN connection. However, for security purposes, on-premises servers are not allowed to access the DNS service on the cloud directly. If your on-premises servers need to access private domain names used within VPCs, or your cloud servers use Huawei Cloud private DNS to access an on-premises domain name, you need to set up DNS on your cloud servers for forwarding DNS queries between the cloud DNS and on-premises DNS. This increases management and maintenance costs and causes reliability risks.

With Huawei Cloud DNS Resolver, on-premises servers and cloud servers can easily communicate with each other in hybrid cloud scenarios.

Figure 3-5 Hybrid cloud DNS resolution



 NOTE

DNS Resolver is now available in CN North-Ulanqab1, CN Southwest-Guiyang1, AP-Bangkok, AP-Singapore, AP-Jakarta, AP-Manila, CN-Hong Kong, AF-Cairo, LA-Sao Paulo1, TR-Istanbul, AF-Johannesburg, ME-Riyadh, and LA-Mexico City2.

Where to Use

- **Access to a Service Domain Name on the Cloud from an On-premises Server**

To enable access, you need to create an inbound endpoint and configure forwarding rules on the on-premises DNS servers to forward the DNS queries for the cloud service domain name to the IP addresses specified in the inbound endpoint.
- **Access to an On-Premises Service Domain Name from a Cloud Server**

To enable access, you need to create an outbound endpoint and configure endpoint rules to specify the on-premises domain name to be accessed and the IP addresses of the on-premises DNS servers. Huawei Cloud private DNS then forwards the DNS queries for the on-premises domain name to the on-premises DNS servers based on the endpoint rules.

Advantages

- Simple networking
You do not need to worry about conflicts with IP addresses starting with 100 because DNS Resolver responds recursively to DNS queries within VPCs.
- Conditional forwarding
DNS queries for particular domain names and for top-level domains are forwarded to specific DNS servers for resolution.

Functions

Table 3-4 Common functions of DNS Resolver

| Function | Description |
|------------------|---|
| Inbound endpoint | Create an inbound endpoint and configure forwarding rules on the on-premises DNS servers to forward the DNS queries for the cloud service domain name to the IP addresses specified in the inbound endpoint. You can create, modify, delete, and view inbound endpoints. For details, see Managing Inbound Endpoints . |

| Function | Description |
|-------------------|--|
| Outbound endpoint | Create an outbound endpoint and configure endpoint rules to specify the on-premises domain name to be accessed and the IP addresses of the on-premises DNS servers. Huawei Cloud private DNS then forwards the DNS queries for the on-premises domain name to the on-premises DNS servers based on the endpoint rules. You can create, modify, delete, and view endpoints, and disassociate endpoints from VPCs. For details, see Managing Outbound Endpoints and Managing Endpoint Rules . |
| Requirements | |

Helpful Links

For details about how to configure DNS Resolver to enable communication between on-premises servers and the cloud, see [Using DNS Resolver to Enable Communication Between On-premises Servers and the Cloud](#).

4 Constraints

Quotas

You can [log in to the console](#) to view the default quota for each resource. To increase the quotas, you can [submit a service ticket](#).

Table 4-1 DNS resource quotas

| Resource Type | Default Quota | How to Increase |
|-------------------|---------------|--|
| Public zone | 50 | Submit a service ticket. |
| Private zone | 50 | Submit a service ticket. |
| Record set | 500 | Submit a service ticket. |
| PTR record | 50 | Submit a service ticket. |
| Custom line | 50 | Submit a service ticket. |
| Inbound endpoint | 50 | Submit a service ticket. |
| Outbound endpoint | 50 | Submit a service ticket. |
| Endpoint rule | 50 | Submit a service ticket. |

Specifications

Table 4-2 DNS specifications

| Resource Type | Specifications | Description |
|---|----------------|--|
| Maximum number of IP addresses that can be bound to an endpoint | 6 | Submit a service ticket to increase the quota. |
| Maximum number of VPCs that can be associated with a private zone | No limit | - |

| Resource Type | Specifications | Description |
|---|------------------|---|
| Maximum number of VPCs that can be associated with an endpoint rule | No limit | - |
| Maximum number of requests for a single ECS in a VPC | 2,000 per second | For a single ECS in a VPC, the maximum number of resolution requests is 2,000 per second. If the number of requests exceeds this, extra requests may not be handled. To avoid this, enable DNS caching to improve lookup efficiency. |
| Total number of requests for all ECSs in a VPC | No limit | - |
| Maximum number of recursive resolution requests for a single ECS in a VPC | 600 per second | For a single ECS in a VPC, the maximum number of external recursive requests is 600 per second. If the number of requests exceeds this, extra requests may not be handled. If your VM requests a swarm of random subdomain names, DNS resolution will be frozen. If your services initiate an enormous volume of concurrent requests, enable DNS caching to improve lookup efficiency. |
| Total number of recursive requests for all ECSs in a VPC | 5,000 per second | For all ECSs in a VPC, the maximum number of external recursive requests is 5,000 per second. If the number of requests exceeds this, extra requests may not be handled. If access to a large number of Internet domain names is required, some domain names may not be accessible due to traffic limiting. To avoid this, submit a service ticket in advance. |

| Resource Type | Specifications | Description |
|---|----------------------------|--|
| Maximum number of recursive resolution requests for a single domain name in a VPC | 50 requests per second | For a single domain name (for example, example.com) and its subdomains in a VPC, the maximum number of external recursive requests is 50 per second. If the number of requests exceeds this, extra requests may not be handled. |
| Bandwidth for handling requests to a public zone | 5 Gbit/s | If your public domain name has abnormal requests evaluated by Huawei, such as attacks, and more than 5 Gbit/s of bandwidth is required for handling the requests, the domain name may be blocked. To address this issue, you should select an appropriate security protection product. |
| Maximum number of requests to a single IP address configured for an inbound endpoint | 10,000 requests per second | Up to 10,000 requests can be routed to a single endpoint IP address per second, and up to 600 external recursive requests can be routed to a public domain name per second. If the number of requests exceeds these limits, extra requests may not be handled. To avoid this, enable DNS caching for your on-premises network to improve lookup efficiency. |
| Maximum number of requests from a single IP address configured for an outbound endpoint | 10,000 requests per second | |

5 Permissions

If you need to assign different permissions to personnel in your enterprise to access your DNS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, fine-grained permissions management, and access control. It helps you secure access to your cloud resources. If your Huawei Cloud account does not require IAM for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account.

With IAM, you can control access to specific Huawei Cloud resources. For example, if you want some software developers in your enterprise to use DNS resources but do not want them to delete DNS resources or perform any other high-risk operations, you can grant permission to use DNS resources but not permission to delete them.

IAM supports role/policy-based authorization and identity policy-based authorization.

The following table describes the differences between these two authorization models.

Table 5-1 Differences between role/policy-based and identity policy-based authorization

| Name | Authorization Using | Permissions | Authorization Method | Scenario |
|-----------------|-------------------------------------|--|--|--|
| Role/Policy | User-permission-authorization scope | <ul style="list-style-type: none"> • System-defined roles • System-defined policies • Custom policies | Assigning roles or policies to principals | To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It is hard to provide fine-grained permissions control using authorization by user groups and a limited number of condition keys. This method is suitable for small- and medium-sized enterprises. |
| Identity policy | Policies | <ul style="list-style-type: none"> • System-defined identity policies • Custom policies | <ul style="list-style-type: none"> • Assigning identity policies to principals • Attaching identity policies to principals | You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises. |

Assume that you want to grant IAM users the permissions needed to create ECSs in CN North-Beijing4 and OBS buckets in CN South-Guangzhou. With role/policy-based authorization, the administrator needs to create two custom policies and assign both to the IAM users. With identity policy-based authorization, the administrator only needs to create one custom policy and configure the condition key **g:RequestedRegion** for the policy, and then attach the policy to the principals or grant the principals the access permissions to the specified regions. Identity policy-based authorization is more flexible than role/policy-based authorization.

Policies and actions in the two authorization models are not interoperable. You are advised to use identity policy-based authorization. For details about system-defined permissions, see [Role/Policy-based Authorization](#) and [Identity Policy-based Authorization](#).

For more information, see [IAM Service Overview](#).

Role/Policy-based Authorization

DNS supports authorization with roles and policies. New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

DNS is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **ap-southeast-2**) in the specified regions (for example, **AP-Bangkok**), the users only have permissions for load balancers in the selected projects. If you set **Scope** to **All resources**, the users have permissions for DNS in all region-specific projects. When accessing DNS, the users need to switch to the authorized region.

Table 5-2 lists all system-defined permissions for DNS. System-defined policies in role/policy-based authorization are not interoperable with those in identity policy-based authorization.

Table 5-2 System-defined permissions for DNS

| Role/Policy Name | Description | Type | Dependencies |
|----------------------|--|-----------------------|--|
| DNS FullAccess | Full permissions for DNS | System-defined policy | None |
| DNS ReadOnlyAccesses | Read-only permissions for DNS. Users granted with these permissions can only view DNS resources. | System-defined policy | None |
| DNS Administrator | Full permissions for DNS | System-defined role | Tenant Guest and VPC Administrator , which must be attached in the same project as the DNS Administrator role |

Table 5-3 lists common operations supported by system-defined permissions for DNS.

Table 5-3 Common operations supported by system-defined permissions

| Operation | DNS FullAccess | DNS ReadOnlyAccesses | DNS Administrator |
|------------------------|----------------|----------------------|-------------------|
| Creating a public zone | Supported | Not supported | Supported |
| Viewing a public zone | Supported | Supported | Supported |

| Operation | DNS FullAccess | DNS ReadOnlyAccess | DNS Administrator |
|---|----------------|--------------------|-------------------|
| Modifying a public zone | Supported | Not supported | Supported |
| Deleting a public zone | Supported | Not supported | Supported |
| Deleting public zones | Supported | Not supported | Supported |
| Disabling or enabling a public zone | Supported | Not supported | Supported |
| Creating a private zone | Supported | Not supported | Supported |
| Viewing a private zone | Supported | Supported | Supported |
| Modifying a private zone | Supported | Not supported | Supported |
| Deleting a private zone | Supported | Not supported | Supported |
| Deleting private zones | Supported | Not supported | Supported |
| Associating a VPC with a private zone | Supported | Not supported | Supported |
| Disassociating a VPC from a private zone | Supported | Not supported | Supported |
| Adding a record set | Supported | Not supported | Supported |
| Viewing a record set | Supported | Supported | Supported |
| Modifying a record set | Supported | Not supported | Supported |
| Deleting a record set | Supported | Not supported | Supported |
| Deleting record sets from multiple public zones | Supported | Not supported | Supported |
| Disabling or enabling a record set | Supported | Not supported | Supported |
| Exporting record sets | Supported | Not supported | Supported |
| Importing record sets | Supported | Not supported | Supported |
| Creating a PTR record | Supported | Not supported | Supported |
| Viewing a PTR record | Supported | Supported | Supported |
| Modifying a PTR record | Supported | Not supported | Supported |
| Deleting a PTR record | Supported | Not supported | Supported |
| Deleting PTR records | Supported | Not supported | Supported |

Identity Policy-based Authorization

DNS supports identity policy-based authorization. [Table 5-4](#) lists all the system-defined policies for DNS in identity policy-based authorization. System-defined policies in identity policy-based authorization are not interoperable with those in role/policy-based authorization.

Table 5-4 System-defined policies for DNS

| Policy Name | Description | Type |
|-------------------------|-------------------------------|--------------------------------|
| DNSFullAccessPolicy | Full permissions for DNS | System-defined identity policy |
| DNSReadOnlyAccessPolicy | Read-only permissions for DNS | System-defined identity policy |

[Table 5-5](#) lists common operations supported by system-defined identity policies for DNS.

Table 5-5 Common operations supported by each system-defined identity policy of DNS

| Operation | DNSFullAccessPolicy | DNSReadOnlyAccessPolicy |
|--|---------------------|-------------------------|
| Creating a public zone | Supported | Not supported |
| Viewing a public zone | Supported | Supported |
| Modifying a public zone | Supported | Not supported |
| Deleting a public zone | Supported | Not supported |
| Deleting public zones | Supported | Not supported |
| Disabling or enabling a public zone | Supported | Not supported |
| Creating a private zone | Supported | Not supported |
| Viewing a private zone | Supported | Supported |
| Modifying a private zone | Supported | Not supported |
| Deleting a private zone | Supported | Not supported |
| Deleting private zones | Supported | Not supported |
| Associating a VPC with a private zone | Supported | Not supported |
| Disassociating a VPC from a private zone | Supported | Not supported |

| Operation | DNSFullAccessPolicy | DNSReadOnlyAccessPolicy |
|---|---------------------|-------------------------|
| Adding a record set | Supported | Not supported |
| Viewing a record set | Supported | Supported |
| Modifying a record set | Supported | Not supported |
| Deleting a record set | Supported | Not supported |
| Deleting record sets from multiple public zones | Supported | Not supported |
| Disabling or enabling a record set | Supported | Not supported |
| Exporting record sets | Supported | Not supported |
| Importing record sets | Supported | Not supported |
| Creating a PTR record | Supported | Not supported |
| Viewing a PTR record | Supported | Supported |
| Modifying a PTR record | Supported | Not supported |
| Deleting a PTR record | Supported | Not supported |
| Deleting PTR records | Supported | Not supported |

Helpful Links

- [IAM Service Overview](#)
- [Using IAM to Grant Access to DNS](#)
- [Actions Supported by Identity Policy-based Authorization](#)

6 Integration with Other Services

Figure 6-1 shows the relationships between DNS and other services.

Figure 6-1 Related services

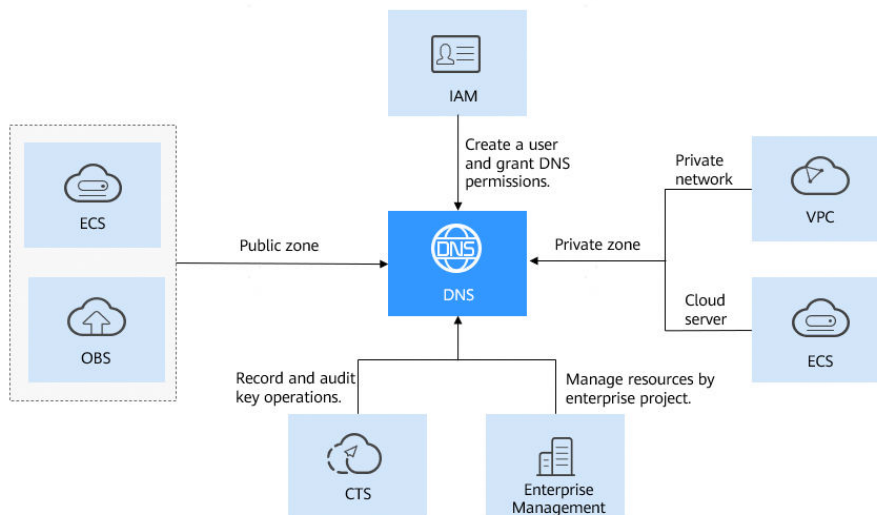


Table 6-1 shows the relationships between DNS and other services.

Table 6-1 DNS and other services

| Related Service | Description | Reference |
|----------------------------|---|---|
| Elastic Cloud Server (ECS) | DNS can resolve the domain names to IP addresses of ECSs where a website or application is deployed so that end users can use domain name to access the website or application. | Routing Internet Traffic to a Website |

| Related Service | Description | Reference |
|------------------------------|--|--|
| Virtual Private Cloud (VPC) | DNS can resolve private domain names that are used for network connections within VPCs. | Routing Traffic in a VPC |
| Object Storage Service (OBS) | DNS maps your domain name to a bucket's access domain name for you to access the static websites hosted in the bucket. | Static Website Hosting |
| Cloud Trace Service (CTS) | CTS can record the operations performed on the DNS service. | DNS Operations Recorded by CTS |
| Enterprise Management | You can create different enterprise projects to manage public zones, private zones, and PTR records. | Creating a Public Zone Creating a Private Zone Creating a PTR Record |

7 Security

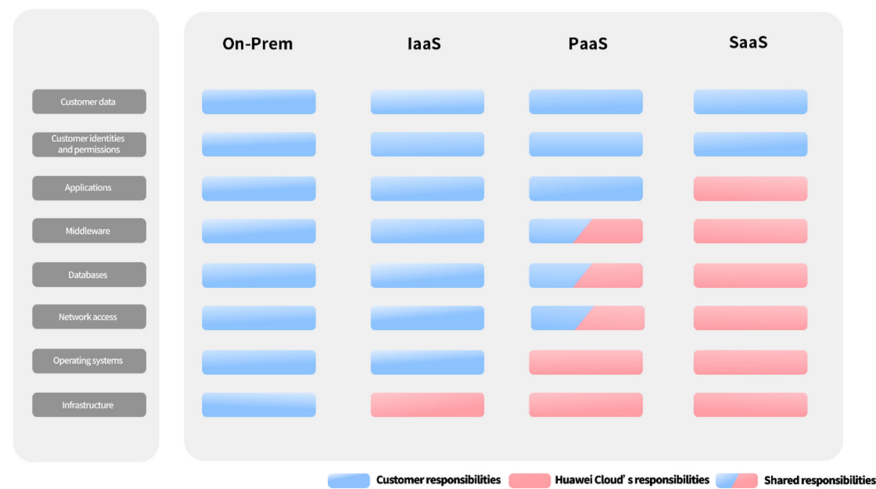
7.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in [Figure 7-1](#).

- **Huawei Cloud:** Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer:** As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 7-1 Huawei Cloud shared security responsibility model



Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in [Figure 7-1](#), customers can select different cloud service types (such as IaaS, PaaS, and SaaS) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the PaaS middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

On-premises (On-Prem): Software and IT infrastructure are deployed and managed by customers within their own data centers, rather than be deployed by remote cloud service providers.

Infrastructure as a Service (IaaS): Cloud service providers offer compute, network, storage, and more infrastructure services, including [Elastic Cloud Server \(ECS\)](#), [Virtual Private Network \(VPN\)](#), and [Object Storage Service \(OBS\)](#).

Platform as a Service (PaaS): Cloud service providers deliver platforms required for application development and deployment, such as [ModelArts](#) and [GaussDB](#). Customers do not need to maintain the underlying infrastructure.

Software as a Service (SaaS): Cloud service providers offer complete application software, such as [Huawei Cloud Meeting](#). Customers use the software directly without the need to install the application, maintain it, or manage its underlying platform or infrastructure.

7.2 Identity and Access Control

You can use Identity and Access Management (IAM) to control access to your DNS 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 DNS to the user group. Then, all users in this group automatically inherit the granted permissions.

For details, see [Permissions Management](#).

7.3 Auditing and Logging

Cloud Trace Service (CTS) is a log audit service for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records to perform security analysis, audit compliance, track resource changes, and locate faults.

After CTS is enabled, traces can be generated for DNS operations.

- For details about how to enable and configure CTS, see [Overview](#).
- For details about key operations of DNS, see [DNS Key Operations Recorded by CTS](#).
- For details about traces, see [Viewing Traces](#).

7.4 Resilience

100+ DNS nodes have been deployed in more than 20 countries and regions around the world. DNS provides multi-AZ, multi-cluster disaster recovery in each region, so even if some nodes, clusters, or regions go down, domain name resolution will not be interrupted. DNS provides service reliability you can count on.

Huawei has more than 10 years of information security experience and has a wealth of excellent practices to rely on. Based on Huawei Cloud's self-built high-security equipment rooms and high-security scrubbing centers on carriers' backbone networks, DNS provides Terabyte-level DDoS protection. It can quickly and effectively cope with various DNS attacks to ensure the continuity of domain name resolution.

Huawei's next-generation Data Plane Development Kit (DPDK) offers higher resolution performance. With DPDK, a single DNS node can support tens of millions of concurrent requests, so DNS can support hundreds of millions of concurrent requests. You get high-performance resolution services with unlimited scalability.

Huawei DNS supports intelligent resolution. User traffic is automatically scheduled to different backend servers by carrier, continent/country, or weight, greatly improving service reliability.

7.5 Monitoring Security Risks

Cloud Eye is a monitoring service from Huawei Cloud. It provides capabilities like real-time monitoring, timely alarm reporting, resource groups, and website monitoring. Cloud Eye helps you keep track of your resource usages and service statuses on the cloud, making it easier to respond to exceptions in a timely manner.

Monitoring is key to ensuring the reliability, availability, and performance of the DNS service. With Cloud Eye, you can view domain name resolution traffic and error logs within your selected time period. You can also dynamically analyze potential risks based on alarms generated.

7.6 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can [download](#) them from the console.

Figure 7-2 Downloading compliance certificates

Download Compliance Certificates

Please enter a keyword to search

BS 10012:2017

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

Download

ENS

Mandatory law for companies in the public sector and their technology suppliers

Download

Singapore Multi Tier Cloud Security (MTCS) Level 3

The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to adopt well-rounded risk management and security practices in cloud computing. The HUAWEI CLOUD Singapore region has obtained the level 3 (highest) certification of MTCS.

Download

Trusted Partner Network (TPN)

The Trusted Partner Network (TPN) is a global, industry-wide media and entertainment content security initiative and community network, wholly owned by the Motion Picture Association. TPN is committed to raising content security awareness and standards and building a more secure future for content partners. TPN can help identify vulnerabilities, increase security capabilities, and efficiently communicate security status to customers.

Download

ISO 27001:2022

ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

Download

ISO 27017:2015

ISO 27017 is an international certification for cloud computing information security. It indicates that HUAWEI CLOUD's information security management has become an international best practice.

Download

Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see [Resource Center](#).

Figure 7-3 Resource center

Resource Center

White Papers

Privacy Compliance White Papers | Industry Regulation Compliance White Papers | Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile, as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China, as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.