**Domain Name Service**

# Service Overview

**Issue**      01
**Date**       2023-07-30

HUAWEI TECHNOLOGIES CO., LTD.

# Contents

# 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 with domain names.

The DNS service is free and is enabled by default.

## Basic Functions

The DNS service provides the following functions:

- **Public domain name resolution**

  Maps domain names to public IP addresses so that end users can access your website or web applications over the Internet.

- **Private domain name 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.

- **Intelligent resolution**

  Returns different IP addresses for the same domain name based on the carrier networks or geographic locations. This significantly reduces network latency for end users from different carrier networks and geographic locations.

## Product Advantages

The DNS service has the following advantages:

- High performance

  A single DNS node can handle millions of concurrent queries, allowing end users to access your website or application more quickly.

- 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**.

- Smooth service migration

  You can migrate an in-use website domain name to the Huawei Cloud DNS service. To ensure that your website services are not interrupted during the migration, we will create a public zone and add DNS record sets for your website in advance.

- 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 enables you to access the DNS service.

  - If you have already registered an account, log in to the management console, hover on the upper left to display **Service List**, and choose **Networking** > **Domain Name Service**.

  - Otherwise, register an account with Huawei Cloud by following the instructions in **Quick Start** and perform the preceding step.

  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 Public Domain Name Resolution

## Public Zone

A public zone contains information about how a domain name and its subdomains are translated into IP addresses for routing traffic over the Internet. Public zones allow end users to access your website or application over the Internet using your domain name.

## Accessing a Website Using a Domain Name

To make your website accessible on the Internet through a domain name, perform the following steps:

1. Register your domain name with a domain name registrar so that end users can use the domain name to access your website.

2. Set up your website.

   Purchase cloud resources from Huawei Cloud or other cloud service providers.

3. Configure the DNS service to route Internet traffic for your domain name.

   Create a public zone to host the domain name on the DNS service and add a record set to map the domain name to the EIP of the server where the website is set up.

   For details, see **Routing Internet Traffic to a Website**.

After you finish the above steps, end users will be able to access your website over the Internet with the registered domain name and its subdomains.

**Figure 2-1** How DNS routes Internet traffic to a website
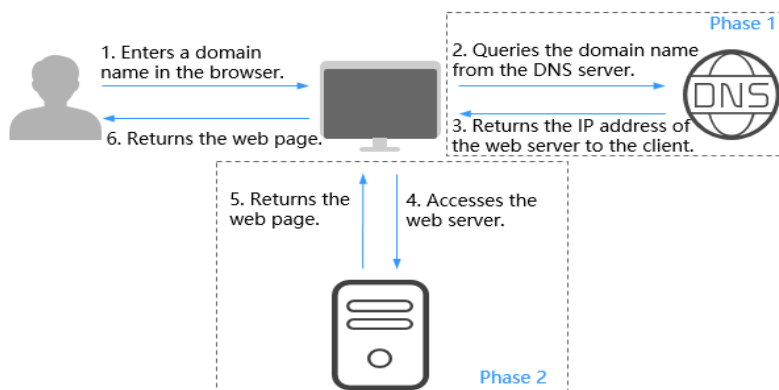


- Phase 1 shows how DNS resolves your domain name.
- Phase 2 shows how the web page is returned to the user.

Public domain name resolution depends on the DNS hierarchy. The following describes the hierarchies of domain names and how domain names are resolved.

## DNS Hierarchy

Domain names are hierarchical, and domain name resolution is a recursive lookup process. The following uses example.com to describe the hierarchies in domain names.

- Root domain

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

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

  Root domain names are resolved by root DNS servers that hold the addresses of top-level DNS 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 DNS servers that hold the addresses of second-level DNS servers. For example, the top-level DNS server of .com saves the addresses of all DNS servers of second-level domain names 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
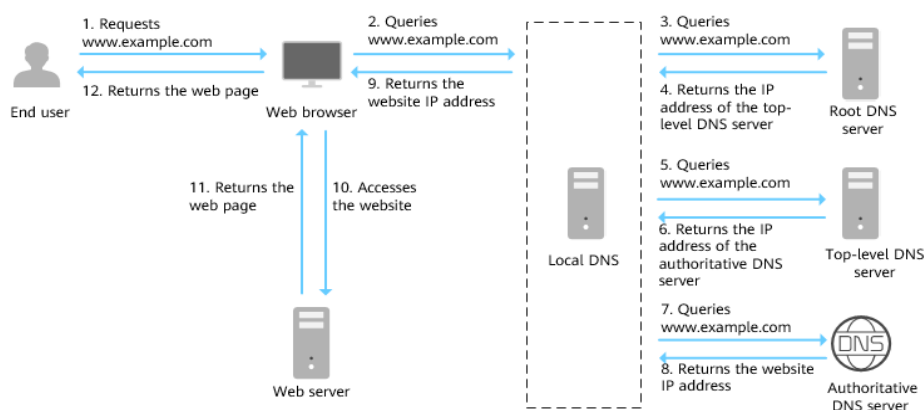
authoritative resolution for example.com, and its address will be recorded by all top-level DNS servers.

If you host domain names on Huawei Cloud DNS, authoritative DNS servers will be provided for the domain names.

## Domain Name Resolution

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

**Figure 2-2** Domain name resolution



1. An end user enters **www.example.com** in the address box of a browser.
2. The request for querying domain name 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 DNS server.
4. The root DNS server returns the DNS server address of .com (because the domain name suffix is .com) to the local DNS server.
5. The local DNS server sends the request to the top-level DNS server of .com.
6. The top-level DNS 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 configure **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.

For details, see **Routing Internet Traffic to a Website**.

# 3 Private Domain Name Resolution

## Private Zone

A private zone contains information about how to map a domain name (such as ecs.com) and its subdomains used within one or more VPCs to private IP addresses (such as 192.168.1.1). With private domain names, your ECSs can communicate with each other within a VPC without having to connect to the Internet. These ECSs can also 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
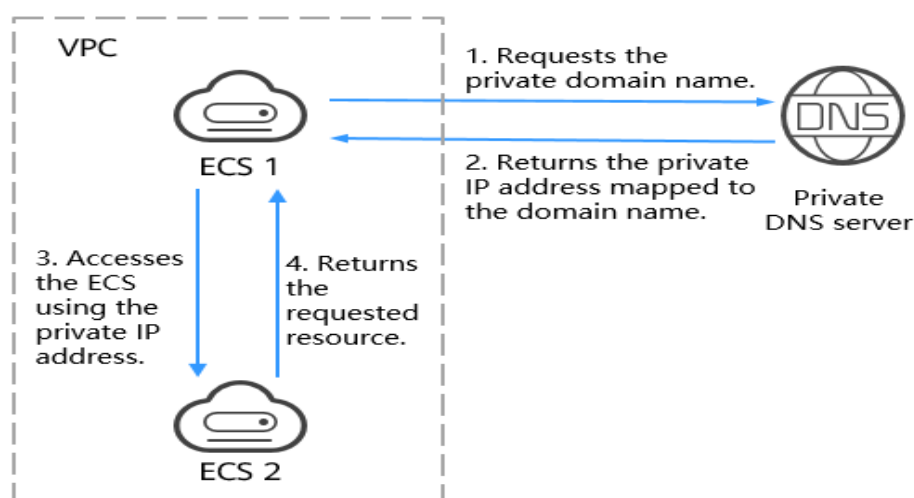


When an ECS in the VPC requests to access a private domain name, the private DNS server directly returns a private IP address mapped to the domain name.

Private zones allow you to:

● Flexibly customize private domain names in your VPCs.

● Associate one or more multiple VPCs with one domain name.

● Use private DNS servers to prevent DNS spoofing and quickly respond to requests for accessing ECSs in VPCs as well as OBS and SMN resources.

You can use private domain names in the following scenarios:

- **Managing ECS Host Names**
- **Keeping Your Website Up and Running Even While Your Server Is Being Replaced**
- **Accessing Cloud Resources**

## Managing ECS Host Names

You can plan host names based on the locations, usages, and account information of ECSs, and map the host names 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 host names (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 host names, you will be able to quickly determine the locations and usages of ECSs during routine management and maintenance.

See **Routing Traffic Within VPCs** for detailed operations.

## 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
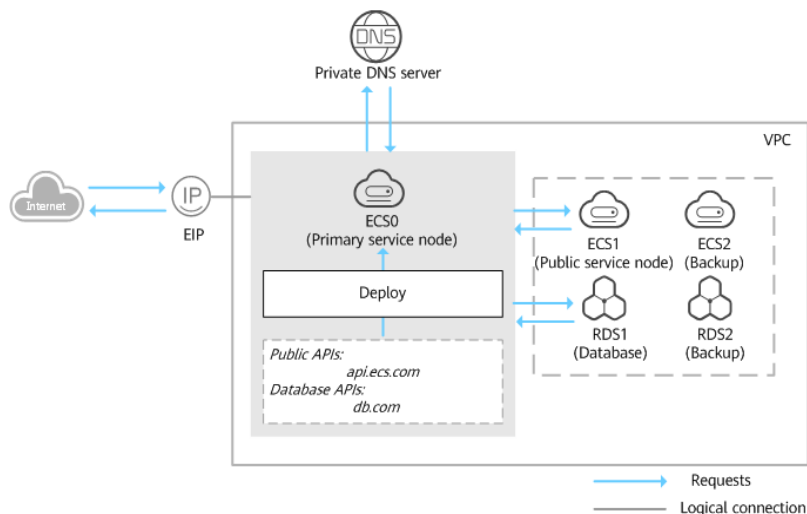


The ECSs and RDS instances are in the same VPC.

- 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.

See **Configuring a Private Domain Name for an ECS** for detailed operations.

## Accessing Cloud Resources

Configure private domain names for ECSs so that they can access other cloud services, such as SMN and OBS, without connecting to the Internet.

When you create an ECS, note the following:

- If a public DNS server is configured for the VPC subnet where the ECS resides, requests to access cloud services will be routed over the Internet.

  **Figure 3-3** shows the process for resolving a domain name when an ECS accesses Huawei cloud services such as OBS and SMN.

  Requests are routed over the Internet, resulting in an increase in network latency.

- If a 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** shows the process.

To make your ECS accessible within the private network, change the default DNS servers of the ECS to private DNS servers, see **How Do I Change Default DNS Servers of an ECS to Private DNS Servers Provided by the DNS Service?**

**Figure 3-3** Accessing cloud services
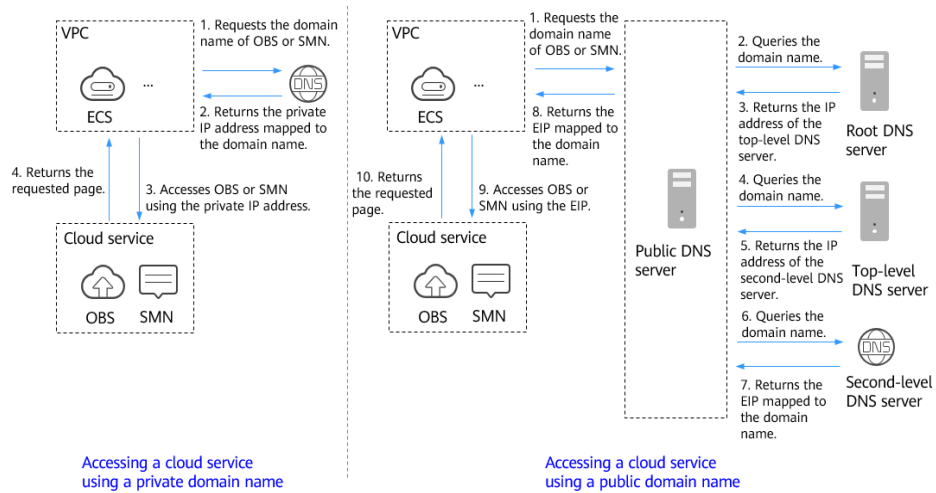
# 4 Reverse Resolution

Reverse resolution, also reverse DNS lookup, resolves an IP address back to a host name. This is typically used to affirm the credibility of email servers.

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 cannot obtain the domain name mapped to the IP address of the sender server, 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 4-1** Reverse resolution
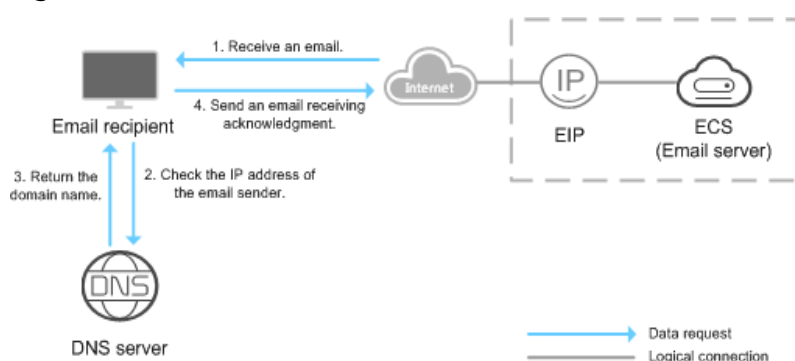


☐ **NOTE**

> **Figure 4-1** shows only the process for reverse resolution. Information about how an email server checks the credibility of the sender's IP address and whether 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.

See **Translating an IP Address to a Domain Name** for detailed operations.

# 5 Intelligent Resolution

If end users access a domain name, DNS servers return the same IP address to the end users regardless of their networks or geographic locations. However, in cross-network or cross-region access, this would lead to an increase in network latency and poor user experience.

With configurable resolution lines, you can specify different IP addresses for the same domain name based on the networks or geographic locations.

You can create more fine-grained resolution lines based on source IP addresses.

Huawei Cloud DNS supports the following types of resolution lines:

- **ISP lines**
- **Region lines**
- **Custom lines**
- **Weighted routing**

📖 NOTE

Resolution lines are not available for private zones and PTR records.

# 6 Functions

Table 6-1 lists basic functions of the DNS service.

Before you use the DNS service, you'd better get familiar with **Product Concepts** to better understand the functions.

**Table 6-1** Common DNS functions

| Category | Function | Description |
|---|---|---|
| Public domain resolution | Public zone | A public zone is used to host a domain name you want to make accessible over the Internet and contains information about how you want to route traffic for the domain name and all its subdomains. You can create, modify, delete, enable, disable, and view public zones.<br><br>For details, see **Public Zone**. |
| | Domain name level | You can create public zones for second-level domain names and their subdomains.<br><br>• For domain names with 1-level suffixes like .com, you can create zones for example.com and www.example.com.<br><br>• For domain names with 2-level suffixes like .com.cn, you can create zones for example.com.cn and www.example.com.cn. |
| | Record set | A record set is a group of resource records that define 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.<br><br>For details, see **Record Set**. |

| Category | Function | Description |
|---|---|---|
| | Regaining a domain name | If a public zone has been created for your domain name by another user, you can regain the domain name by proving that you are the holder of this domain name.<br><br>For details, see **Regaining a Domain Name**. |
| | Wildcard resolution | You can add record sets for all subdomains of a second-level domain name.<br><br>For details, see **Creating a Wildcard DNS Record Set**. |
| | TTL | TTL is short for time to live, which specifies the cache period of resource records on a local DNS server, in seconds. The TTL value ranges from **1** to **2147483647**. |
| | Weight | Weight indicates the proportion of DNS queries that will be routed to the record set.<br><br>If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set.<br><br>For details, see **Configuring Weighted Routing**. |
| | Batch operation | You can delete multiple public zones at a time. |
| Private domain name resolution | Private zone | A private zone is used to host private domain names that are used in VPCs. You can create, modify, delete, and view private zones, associate private zones with VPCs, and disassociate private zones from VPCs.<br>● Private zones can be created without the need to register domain names.<br>● Each private zone must be unique in the associated VPC.<br><br>For details, see **Private Zone**. |
| | Associating a private zone with or disassociating a private zone from a VPC | You can associate a private zone with a VPC or disassociate a private zone from a VPC.<br><br>For details, see **Associating a VPC with a Private Zone** and **Disassociating a VPC from a Private Zone**. |

| Category | Function | Description |
|---|---|---|
|  | Record set | A record set is a group of resource records that define 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.<br><br>For details, see **Record Set**. |
|  | Wildcard resolution | You can add record sets for all subdomains of a private domain name. DNS provides resolution services for all subdomains.<br><br>For details, see **Creating a Wildcard DNS Record Set**. |
|  | TTL | TTL is short for time to live, which specifies the cache period of resource records on a local DNS server, in seconds. The TTL value ranges from **1** to **2147483647**. |
|  | Batch deleting private zones | You can delete multiple private zones at a time. |
| Reverse resolution | PTR record | Reverse resolution involves obtaining a domain name based on an IP address. This function is useful when you want to build an email server. You can create, modify, and delete PTR records.<br><br>For details, see **PTR Record**. |
|  | TTL | TTL is short for time to live, which specifies the cache period of resource records on a local DNS server, in seconds. The TTL value ranges from **1** to **2147483647**. |
| Intelligent resolution | ISP line | DNS can return the optimal IP addresses to end users based on the carrier networks they use.<br><br>For details, see **Configuring ISP Lines**. |
|  | Region line | DNS can return the optimal IP addresses to end users based on their geographic locations.<br><br>For details, see **Configuring Region Lines**. |

| Category | Function | Description |
|---|---|---|
| Record set | Searching for record sets globally | DNS allows you to centrally manage record sets in both public and private zones, including the following:<br><br>• Searching for record sets by status, type, name, value, ID, or tag<br>• Modifying, deleting, disabling, or enabling record sets in public zones<br>• Modifying or deleting record sets in private zones<br><br>For details, see **Searching for Record Sets**. |
| | Batch deleting private zones | You can import, export, and delete record sets in both public and private zones in batches.<br><br>For details, see **Importing Record Sets** and **Exporting Record Sets**. |
| Auditing | Viewing audit logs | With CTS, you can record operations associated with DNS for later query, audit, and backtrack operations.<br><br>Huawei Cloud allows you to **view audit logs**, and you can view and export operation records of the last seven days on the CTS console. |
| Tag | Resource tag | You can configure tags for public zones, private zones, record sets, and PTR records. You can also use **predefined tags** of TMS to quickly associate tags with resources. |
| Quota | Quota adjustment | Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number and capacity of resources available to end users, for example, how many public zones, private zones, record sets, and PTR records you can create.<br><br>If the existing resource quotas cannot meet your service requirements, you can request higher quotas.<br><br>For details, see **Quota Adjustment**. |

# 7 Constraints

## Resource Quotas

**Table 7-1** lists the DNS resource quotas.

**Table 7-1** DNS resource quotas

| Resource | Default Quota | Adjustable |
|---|---|---|
| Public zone | 50 | **Submit a service ticket**. |
| Private zone | 50 | |
| Record set | 500 | |
| PTR record | 50 | |
| Custom line | 50 | |
| Maximum number of VPCs that can be associated with a private zone | Unlimited | - |
| Maximum number of VPCs that can be associated with a resolution rule | Unlimited | - |

# 8 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, permissions management, and access control, helping you to securely access your resources.

With IAM, you can create IAM users and assign permissions to control their access to specific 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 create IAM users and grant permission to use DNS resources but not permission to delete them.

If your Huawei Cloud account does not require individual IAM users for permissions management, you can skip this section.

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

For more information about IAM, see **IAM Service Overview**.

## DNS Permissions

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 resources include the following:

- Public zone: global-level resource
- Private zone: project-level resource
- PTR record: project-level resource

DNS permissions for global-level resources cannot be set in the global service project and must be granted for each project.

When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **eu-west-101**) in the specified regions (for example, **EU-Dublin**), the users only have permissions for DNS 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.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Huawei Cloud services depend on each other. When you grant permissions using roles, you also need to attach dependent roles. Roles are not ideal for fine-grained authorization and least privilege access.

- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permissions to manage DNS resources of a certain type. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by DNS, see **Permissions and Supported Actions**.

**Table 8-1** lists system-defined permissions supported by DNS.

**Table 8-1** System-defined permissions for DNS

| Role/Policy Name | Description | Type | Dependencies |
|---|---|---|---|
| DNS FullAccess | Full permissions for DNS | System-defined policy | None |
| DNS ReadOnlyAccess | 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 8-2** lists common operations supported by system-defined permissions for DNS.

**Table 8-2** Common operations supported by system-defined permissions

| Operation | DNS FullAccess | DNS ReadOnlyAccess | 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 in batches | 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 in batches | 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 |
| Modify a record set | Supported | Not supported | Supported |
| Deleting a record set | Supported | Not supported | Supported |
| Delete record sets in batches | Supported | Not supported | Supported |
| Disabling or enabling a record set | Supported | Not supported | Supported |
| Exporting record sets in batches | Supported | Not supported | Supported |
| Importing record sets in batches | 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 |

| Operation | DNS FullAccess | DNS ReadOnlyAccess | DNS Administrator |
|---|---|---|---|
| Deleting PTR records in batches | Supported | Not supported | Supported |

## Helpful Links

- **What Is IAM?**
- **Creating a User and Granting DNS Permissions**
- **Permissions Policies and Supported Actions**

# 9 Integration with Other Services

**Figure 9-1** shows the relationships between DNS and other services.
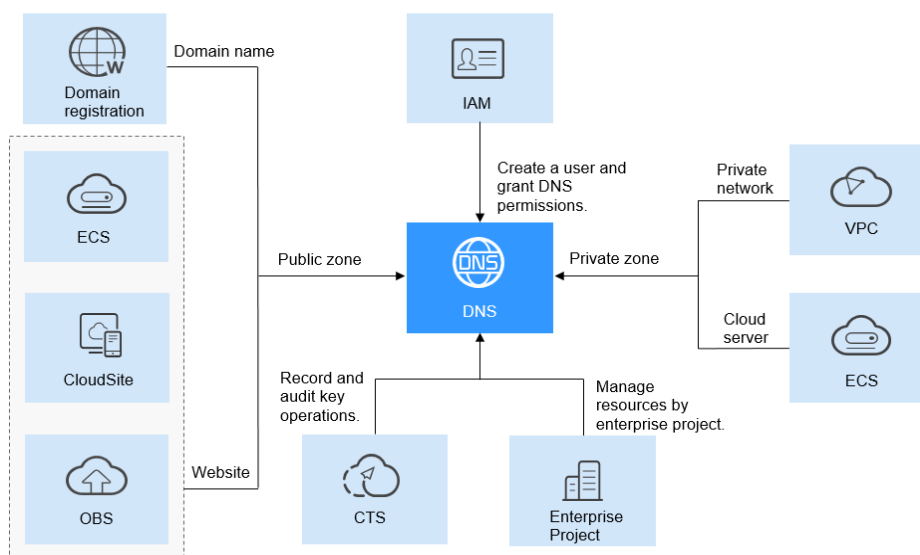
**Figure 9-1** Related services



**Table 9-1** shows the relationships between DNS and other services.

**Table 9-1** 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 Within VPCs** |
| 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** <br> **Creating a Private Zone** <br> **Creating a PTR Record** |

# 10 Product Concepts

## 10.1 Domain Name Format and DNS Hierarchy

A valid domain name meets the following requirements:

- A domain name is segmented using dots (.) into multiple labels.
- A domain name label can contain specified characters in different languages, letters, digits, and hyphens (-) and cannot start or end with a hyphen.
- A label cannot exceed 63 characters.
- The total length of a domain name, including the dot at the end, cannot exceed 254 characters.

A domain name is divided into the following levels based on its structure:

- Root domain: . (a dot)
- Top-level domain: for example, .com, .net, .org, and .cn
- Second-level domain: subdomains of the top-level domain names, such as example.com, example.net, and example.org
- Third-level domain: subdomains of the second-level domain names, such as abc.example.com, abc.example.net, and abc.example.org
- The next-level domain names are similarly expanded by adding prefixes to the previous-level domain names, such as def.abc.example.com, def.abc.example.net, and def.abc.example.org.

## 10.2 Record Set

### Overview

A record set is a collection of resource records that belong to the same domain name. A record set defines DNS record types and values.

If you have created a zone on the DNS console, you can create record sets to expand the domain name or record its detailed information.

**Table 10-1** describes the record set types and their application scenarios.

**Table 10-1** Record set usages

| Type | Where to Use | Description |
|---|---|---|
| A | Public and private zones | Maps domains to IPv4 addresses. |
| CNAME | Public and private zones | Maps one domain name to another domain name or multiple domain names to one domain name. |
| MX | Public and private zones | Maps domain names to email servers. |
| AAAA | Public and private zones | Maps domain names to IPv6 addresses. |
| TXT | Public and private zones | TXT record sets are usually used to record the following:<br>● DKIM public keys to prevent email fraud<br>● The identity of domain name owners to facilitate domain name retrieval |
| SRV | Public and private zones | Records servers providing specific services. |
| NS | Public and private zones | Delegates subdomains to other name servers.<br>● For public zones, an NS record set is automatically created, and you can add NS record sets for subdomains.<br>● For private zones, an NS record set is automatically created, and you cannot add other NS record sets. |
| SOA | Public and private zones | Identifies the base information about a domain name. The SOA record set is automatically generated by the DNS service and cannot be added manually. |
| CAA | Public zone | Grants certificate issuing permissions to CAs. CAA record sets can prevent the issuance of unauthorized HTTPS certificates. |
| PTR | Public and private zones | Maps IP addresses to domain names. |

## Usage

Record sets are used in following scenarios:

● Routing Internet traffic to a website

A and AAAA record sets are usually used to map domain names used by websites to IPv4 or IPv6 addresses of web servers where the websites are deployed.

**Figure 10-1** Accessing a website over the Internet using domain name



- Private domain name resolution

  On a private network, A and AAAA record sets translate private domain names into private IP addresses.

**Figure 10-2** Private domain name resolution



- Email domain name resolution

  MX, CNAME, and TXT record sets are usually used for email services.

**Figure 10-3** Email domain name resolution
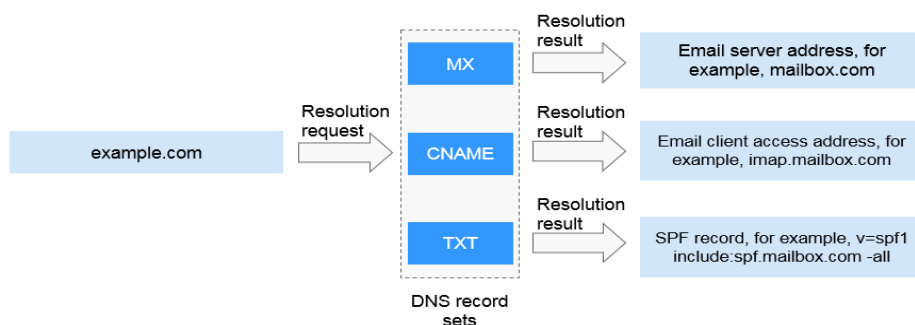


- Reverse resolution on a private network

  PTR records translate private IP addresses into private domain names.

**Figure 10-4** Reverse resolution on a private network



## Helpful Links

For details about how to add and manage record sets, see **Record Set**.

# 10.3 Region and AZ

## Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.

- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. to support high-availability systems.

## Selecting a Region

If your target users are in Europe, select the **EU-Dublin** region.

## Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

# 10.4 Project

Projects are used to group and isolate cloud resources, including computing, storage, and network resources. Multiple projects can be created for one account. A project can be a department or a project team.

Public zones are global-level resources, while private zones and PTR records are resources at the region level. 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.