Domain Name Service

User Guide

Issue   01
Date   2023-11-30

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Overview

1.1 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.

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.

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.

- 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.

  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*.

1.2 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.

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 1-1 How DNS routes Internet traffic to a website
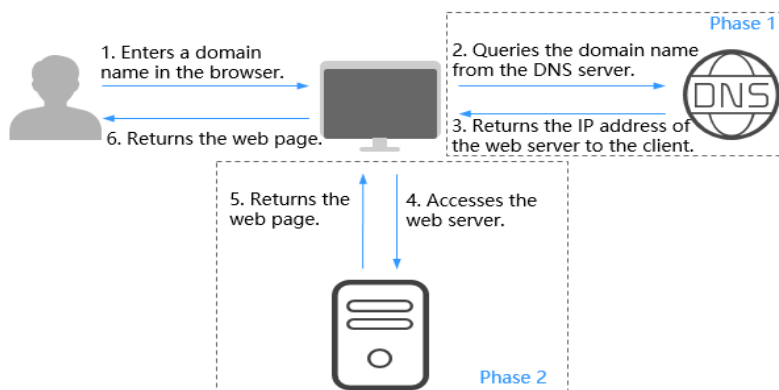
- Phase 1 shows how DNS resolves your domain name.
- Phase 2 shows how the web page is returned to the user.

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 DNS, authoritative DNS servers will be provided for the domain names.

Domain Name Resolution

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

Figure 1-2 Domain name resolution
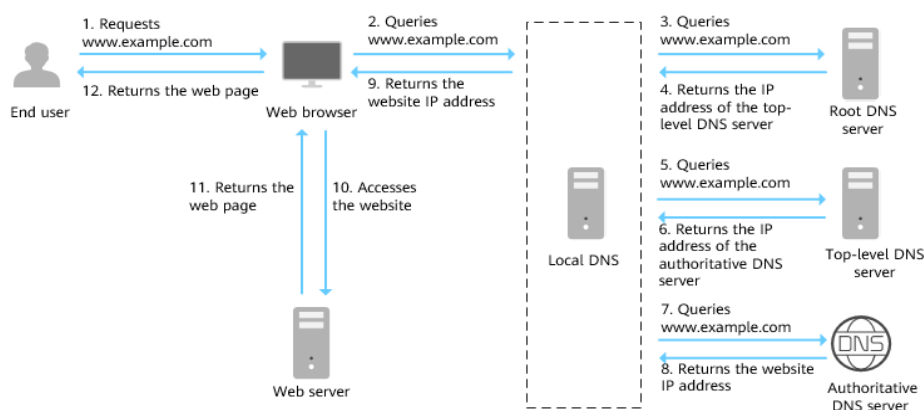
1. An end user enters **www.example.com** in the address box of a browser.

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 the name servers provided by the DNS service, 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**.

1.3 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 1-3 shows how a private domain name is resolved by a private DNS server.

Figure 1-3 Process for resolving a private domain name
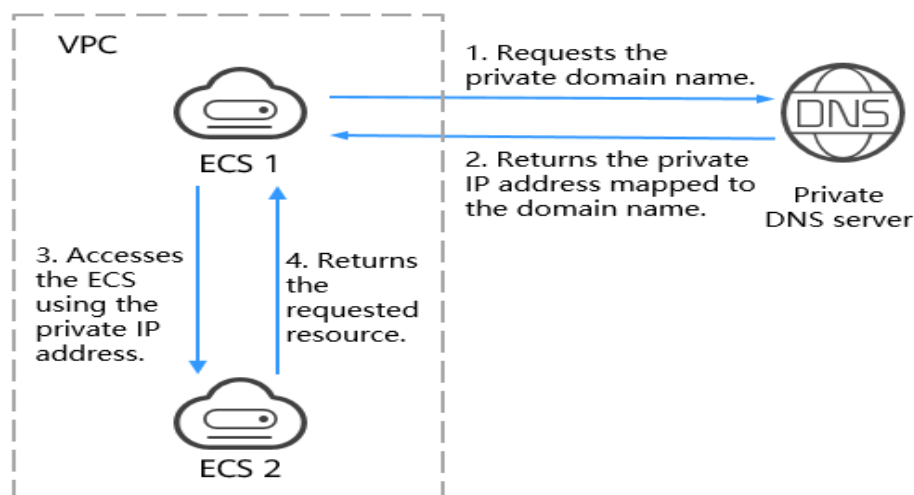
When an ECS in the VPC requests to access a private domain name, the private DNS server directly returns a private IP address mapped to the domain name.

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 1-4 illustrates such use of private domain name resolution.

Figure 1-4 Configuring private DNS for cloud servers
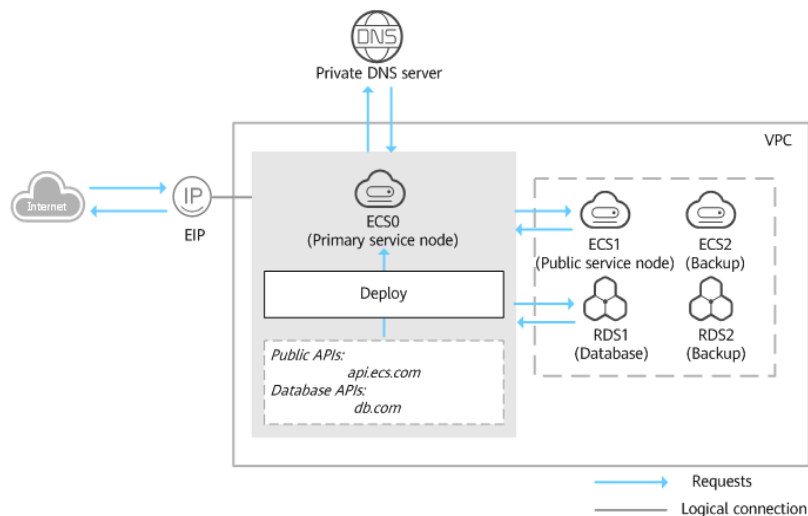
The ECSs and RDS instances are in the same VPC.

- 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.

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 1-5 shows the process for resolving a domain name when an ECS accesses 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 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 1-5** shows the process.

Figure 1-5 Accessing cloud services
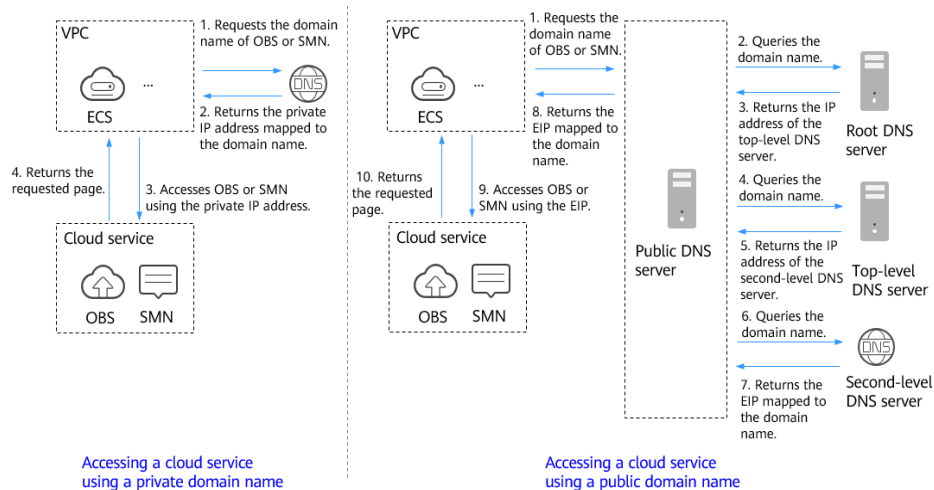
1.4 Reverse Resolution

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 1-6 Reverse resolution
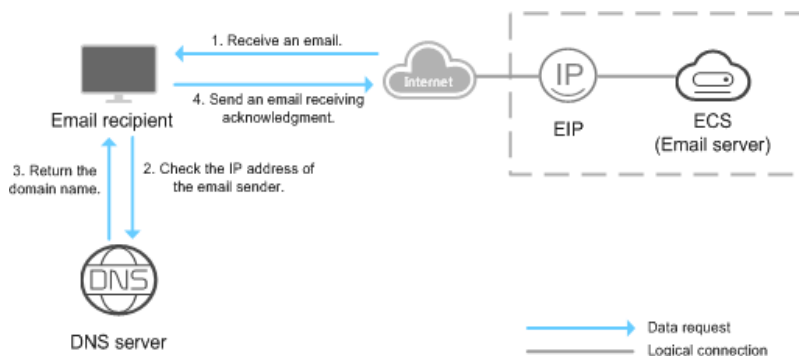
> **NOTE**
>
> **Figure 1-6** shows only the process for reverse resolution. Information about how an email server checks the credibility of the sender's IP address and whether domain name is available on the Internet is not provided here.

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.

1.5 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, permissions management, and access control, helping you to securely access your cloud 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 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 in the specified regions, 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. 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" in the *Domain Name Service API Reference*.

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

Table 1-1 System-defined permissions for DNS

Role/Policy Name	Description	Type	Dependencies
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 1-2 lists common operations supported by system-defined permissions for DNS.

Table 1-2 Common operations supported by system-defined permissions

Operation	DNS Administrator	DNS ReadOnlyAccess
Creating a public zone	Supported	x
Viewing a public zone	Supported	Supported
Modifying a public zone	Supported	x
Deleting a public zone	Supported	x
Creating a private zone	Supported	x
Viewing a private zone	Supported	Supported
Modifying a private zone	Supported	x
Deleting a private zone	Supported	x
Associating a VPC with a private zone	Supported	x
Disassociating a VPC from a private zone	Supported	x
Adding a record set	Supported	x

Operation	DNS Administrator	DNS ReadOnlyAccess
Viewing a record set	Supported	Supported
Modify a record set	Supported	x
Deleting a record set	Supported	x
Creating a PTR record	Supported	x
Viewing a PTR record	Supported	Supported
Modifying a PTR record	Supported	x
Deleting a PTR record	Supported	x

Helpful Links

- **IAM Service Overview**
- **Creating a User and Granting DNS Permissions**
- "Permissions Policies and Supported Actions" in the *Domain Name Service API Reference*

1.6 Integration with Other Services

Figure 1-7 Related services
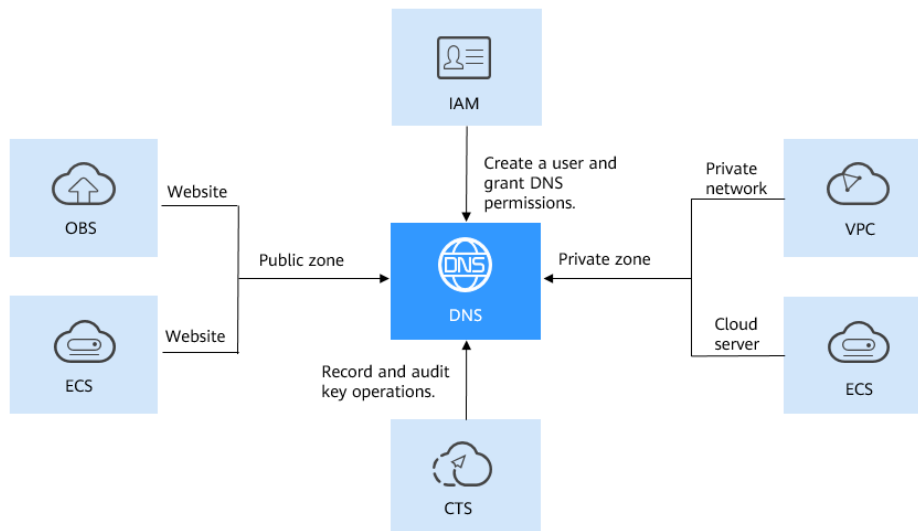
Table 1-3 shows the relationships between DNS and other services.

Table 1-3 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**
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 resolves domain names configured for static website hosting in OBS.	**Using a User-Defined Domain Name to Host a Static Website**
Cloud Trace Service (CTS)	CTS can record the operations performed on the DNS service.	**DNS Operations Recorded by CTS**
Identity and Access Management (IAM)	You can create IAM users and grant the permissions of the DNS service to these users .	**Creating a User and Granting DNS Permissions**

1.7 Product Concepts

1.7.1 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 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.

1.7.2 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 1-4 describes the record set types and their application scenarios.

Table 1-4 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: - DKIM public keys to prevent email fraud - 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. - For public zones, an NS record set is automatically created, and you can add NS record sets for subdomains. - For private zones, an NS record set is automatically created, and you cannot add other NS record sets.

Type	Where to Use	Description
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 1-8 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 1-9 Private domain name resolution

- Email domain name resolution

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

  Figure 1-10 Email domain name resolution
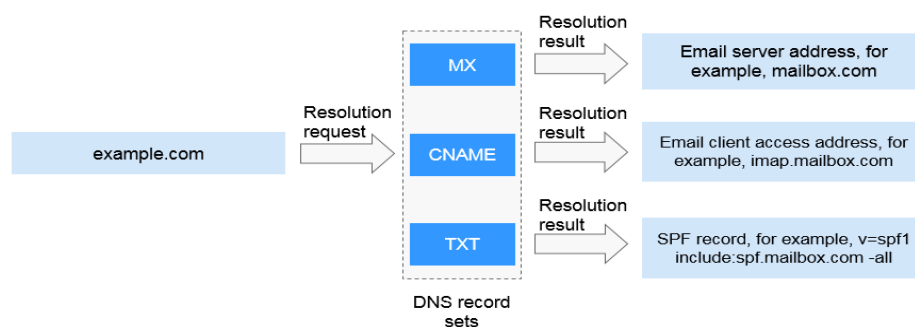
● Reverse resolution on a private network

PTR records translate private IP addresses into private domain names.

Figure 1-11 Reverse resolution on a private network
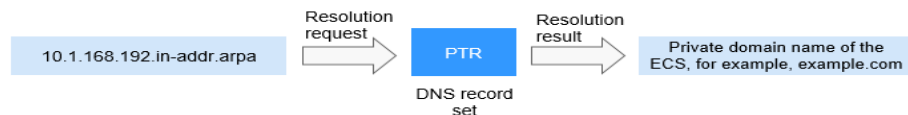
Helpful Links

For details, see **Record Set Overview**.

1.7.3 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.

● A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.

● An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-12 shows the relationship between regions and AZs.

Figure 1-12 Regions and AZs
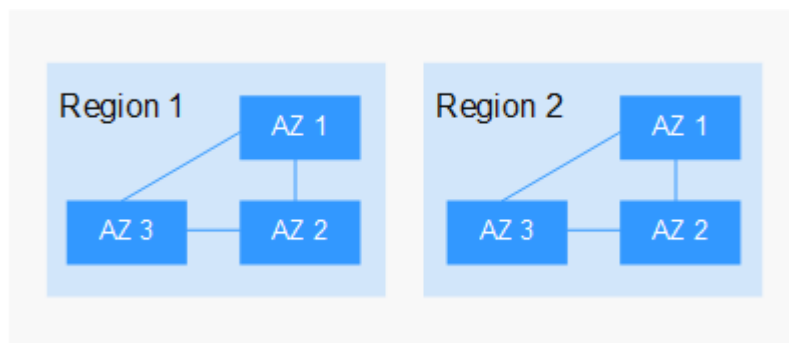
Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

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.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

1.7.4 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.

2 Getting Started

2.1 Before You Start

DNS provides a set of functions for different scenarios.

When DNS Is Required

You can select a type of function based on **Table 2-1** to suit your network scenario.

Table 2-1 Scenarios where DNS is required

Function	Scenario	Reference
Public domain name resolution	Domain names are mapped to the public IP addresses of web servers or web applications on the Internet so that end users are routed to your website or application.	**Routing Internet Traffic to a Website**
Private domain name resolution	Domain names are mapped to the private IP addresses within the VPCs for accessing cloud resources or cloud services over a private network.	**Routing Traffic Within VPCs**
Reverse resolution	EIPs are mapped to domain names, which is often used by email servers against spammers.	**Translating an IP Address to a Domain Name**

2.2 Routing Internet Traffic to a Website

Scenario

After you register a domain name and set up a website, you can configure record sets to map the domain name to the public IP address of the web server so that end users can use the domain name to access your website over the Internet.

For example, you have already built a website on a web server with a public IPv4 address bound. To allow end users to access your website using domain name example.com and its subdomain www.example.com, perform the following operations:

- Add an A record set that maps domain name example.com to the public IP address of the web server.
- Add an A record set that maps subdomain www.example.com to the public IP address of the web server.

Prerequisites

- You have registered domain name example.com.
- You have deployed a web server and obtained its public IP address.

Process Flow

Figure 2-1 shows the process for configuring a domain name for your website.

Figure 2-1 Process for configuring a domain name
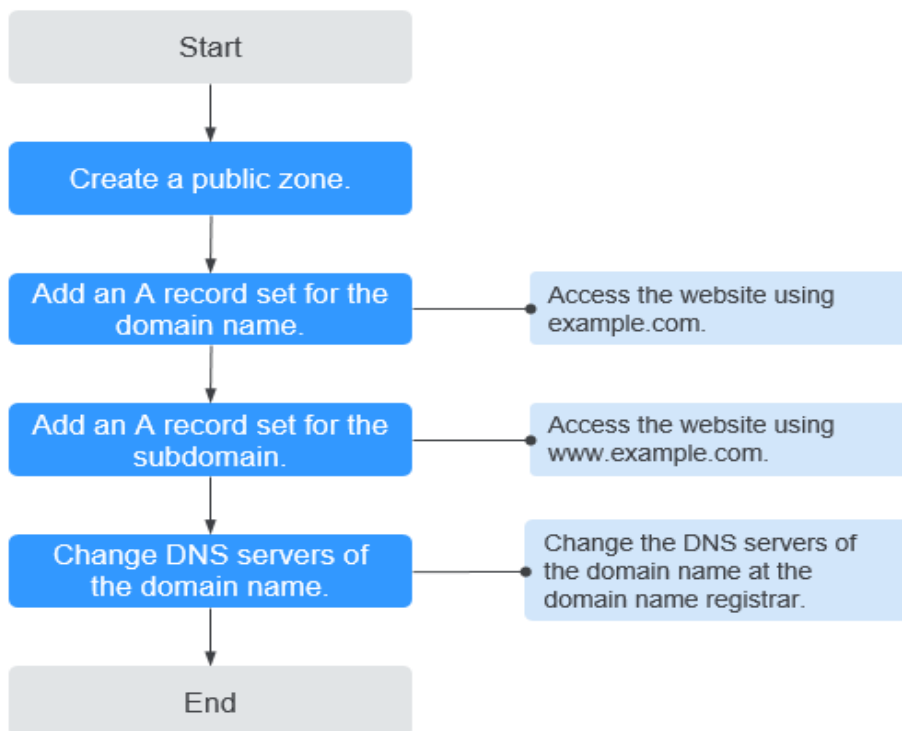
Procedure

Step 1 Create a public zone.

Create a public zone for your domain name on the DNS console.

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Public Zones**.
   The **Public Zones** page is displayed.
4. Click **Create Public Zone**.
5. Set **Domain Name** to **example.com**.
   Configure other parameters by referring to **Creating a Public Zone**.
6. Click **OK**.
   You can view the created public zone on the **Public Zones** page.

   📖 **NOTE**

   You can click the domain name to view SOA and NS record sets automatically generated for the zone.
   – The NS record set defines the authoritative DNS servers for the domain name.
   – The SOA record set identifies the primary authoritative server for the domain name.

Step 2 Add an A record set to the second-level domain name.

Add an A record set to the created public zone to allow access to your website using example.com.

1. On the **Public Zones** page, click the domain name (**example.com**) of the public zone you created.
   The **Record Sets** page is displayed.
2. Click **Add Record Set**.
3. Configure the parameters as follows:
   – **Name**: Leave this parameter blank. The DNS service automatically considers example.com as the name, and requests are routed to example.com.
   – **Type**: Retain the default setting **A – Map domains to IPv4 addresses**.
   – **Value**: Enter the public IP address of your web server.
   Configure other parameters by referring to **Adding an A Record Set**.
4. Click **OK**.
   You can view the added record set in the **Normal** state.

Step 3 Add an A record set to a subdomain.

Add another A record set to the created public zone to allow access to your website using www.example.com.

1. On the **Public Zones** page, click the domain name (**example.com**) of the public zone you created.

The **Record Sets** page is displayed.

2. Click **Add Record Set**.

3. Configure the parameters as follows:
   – **Name**: Set it to **www**, indicating that the subdomain to be resolved is **www.example.com**.
   – **Type**: Retain the default setting **A – Map domains to IPv4 addresses**.
   – **Value**: Enter the public IP address of your web server.

   Configure other parameters by referring to **Adding an A Record Set**.

4. Click **OK**.

   You can view the added record set in the **Normal** state.

Step 4 Change the DNS server addresses.

The DNS service provides authoritative DNS servers for domain resolution.

After you create a public zone, an NS record set is generated, which specifies the DNS servers provided by the DNS service.

If DNS server addresses of the public domain name are not the same as those in the NS record set, the DNS service will not be able to resolve the domain name. You must change the DNS server addresses of the domain name on the registrar's website.

📖 **NOTE**

Generally, the changes to DNS server addresses take effect within 48 hours, but the time may vary depending on the domain name registrar's cache duration.

Query the DNS server addresses provided by the DNS service.

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.

3. In the navigation pane on the left, choose **Public Zones**.
   The **Public Zones** page is displayed.

4. Click the domain name of the public zone you created.
   Locate the NS record set and view the DNS server addresses under **Value**.

Change the DNS servers.

Log in to the domain name registrar's website and change the DNS server addresses to those provided by the DNS service. Refer to the domain name registrar's documentation for detailed operations.

----End

2.3 Routing Traffic Within VPCs

Scenario

If you have deployed ECSs and other cloud services within VPCs, you can configure private domain names for the ECSs so that they can communicate with each other or access the cloud services over a private network.

You can create any private zones that are unique within VPCs. You do not need to register the domain names.

Prerequisites

You have created an ECS and obtained its VPC name and private IP address.

Process Flow

Figure 2-2 shows the process of configuring a private zone for routing traffic within VPCs.

Figure 2-2 Configuring a private zone for routing traffic within VPCs
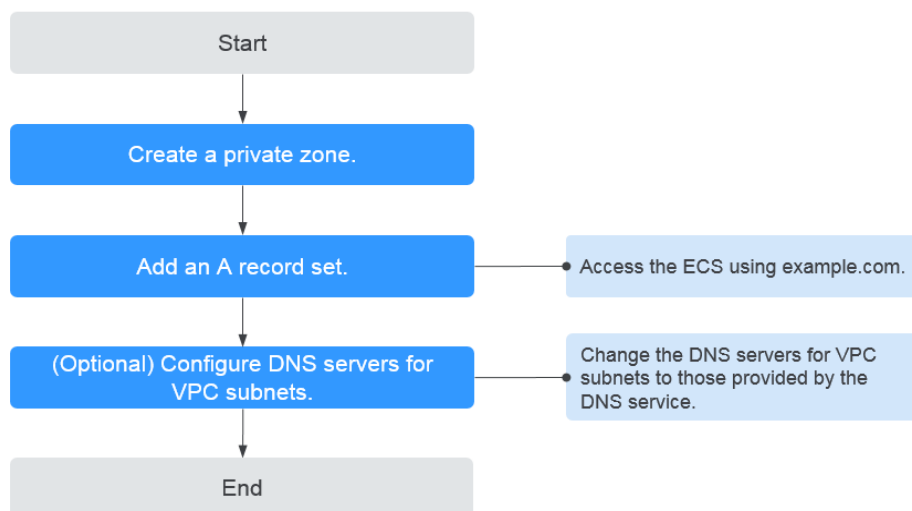
NOTE

To ensure that the private domain name can be resolved in the associated VPC, verify that the DNS server addresses for the VPC subnet are those provided by the DNS service. If the DNS server addresses are not those provided by the DNS service, change them.

You can also **change the DNS server addresses of the VPC subnet** where the domain name is used.

Creating a Private Zone

Step 1 Create a private zone.

Create a private zone to allow access to your ECS using a private domain name example.com.

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Private Zones**.

   The **Private Zones** page is displayed.

4. Click ⊙ in the upper left corner and select the desired region and project.

5. Click **Create Private Zone**.

6. Set **Domain Name** to **example.com** and select the VPC where the ECS resides.

   For details about more parameters, see **Creating a Private Zone**.

7. Click **OK**.

8. Switch back to the **Private Zones** page.

   You can view the created private zone in the list.

   📖 **NOTE**

   Click the domain name to view SOA and NS record sets automatically generated for the zone.
   – The SOA record set identifies the primary authoritative server for the domain name.
   – The NS record set defines the authoritative DNS servers for the domain name.

Step 2 Add an A record set to the domain name.

To access the ECS using example.com, add an A record set.

1. On the **Private Zones** page, click the domain name of the private zone you created.

   The **Record Sets** page is displayed.

2. Click **Add Record Set**.

3. Configure the parameters as follows:

   – **Name**: Leave this parameter blank. The DNS service automatically considers example.com as the name, and requests are routed to example.com.

   – **Type**: Retain the default setting **A – Map domains to IPv4 addresses**.

   – **Value**: Enter the private IP address of the ECS.

   Configure other parameters by referring to **Adding an A Record Set**.

4. Click **OK**.

5. Switch back to the **Record Sets** tab.

   You can view the added record set in the **Normal** state.

Step 3 Change the DNS server addresses of the VPC subnet.

To ensure that the private domain name can be resolved in the associated VPC, verify that the DNS server addresses for the VPC subnet are those provided by the DNS service. If the DNS server addresses are not those provided by the DNS service, change them.

Query the private DNS server addresses provided by the DNS service.

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click ⊙ in the upper left corner and select the desired region and project.
5. In the private zone list, click the domain name of the zone and view the DNS server addresses.

Change the DNS server addresses.

1. Go to the private zone list.
2. Click the VPC name under **Associated VPC**.
   On the VPC console, change the DNS server addresses for the VPC subnet.
   For details, see the *Virtual Private Cloud User Guide*.

   ----End

2.4 Translating an IP Address to a Domain Name

Scenario

PTR records are used to prove credibility of IP addresses and domain names of email servers. To avoid being tracked, most spam senders use email servers whose IP addresses are dynamically allocated or not mapped to registered domain names. If you want to keep the spam out of your recipients' inbox, add a PTR record to map the email server IP address to a domain name. In this way, the email recipients can obtain the domain name by IP address and will know that the email server is trustworthy.

If you use an ECS as an email server, configure a PTR record to map the EIP of the ECS to the domain name.

This following are operations for you to add a PTR record for a cloud resource, such as ECS.

Constraints

You can only configure PTR records for IP addresses with a 32-bit subnet mask.

Prerequisites

- You have registered a domain name.
- You have created an ECS and bound an EIP to it.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **PTR Records**.

   The **PTR Records** page is displayed.

4. Click ⊙ in the upper left corner and select the desired region and project.

5. Click **Create PTR Record** and configure the following parameters.

   – **EIP**: Select the EIP of the ECS.

   – **Domain Name**: Enter the domain name that the EIP points to.

   Configure other parameters by referring to **Creating a PTR Record**.

6. Click **OK**.

   You can view the created PTR record on the **PTR Records** page.

   📖 **NOTE**

   > If a domain name is mapped to multiple EIPs, you must create a PTR record for each EIP.

7. Verify that the PTR record has taken effect by running the following command on a PC connected to the Internet:

   nslookup -qt=ptr *EIP*

3 Public Zones

3.1 Overview

A public zone provides information to translate a domain name and its subdomains into IP addresses required for network communications over the Internet. Visitors can access your website by entering a domain name in the address box of a browser. To use DNS for public domain name resolution, create a public zone for your domain name, and add record sets to map your domain name to one or more IP addresses.

Table 3-1 describes the operations required for creating and managing public zones.

Table 3-1 Public zone operations

Operation	Scenario	Constraints
Creating a Public Zone	Create a zone for your domain name.	- Public zones are global resources. You do not need to select a region or project. - Each account can have up to 50 public zones. - The domain name can be a second-level domain name (for example, example.com) or one of its subdomains (for example, abc.example.com).
Managing Public Zones	Modify, delete, and view public zones.	- The domain name of a created public zone cannot be modified. - If a public zone is deleted, all its record sets will also be deleted.

3.2 Creating a Public Zone

Scenarios

Create a public zone for your domain name on the DNS console.

Prerequisites

You have registered a domain name.

Procedure

If your domain name is registered with a third-party registrar, create a public zone and add record sets to it on the DNS console.

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Public Zones**.

   The **Public Zones** page is displayed.

4. Click **Create Public Zone**.

5. Configure the parameters.

   Table 3-2 describes the parameters.

   Table 3-2 Parameters for creating a public zone

Parameter	Description	Example Value
Domain Name	Domain name you registered.	example.com
Email	(Optional) Email address of the administrator managing the public zone. Recommended email address: **HOSTMASTER@*Domain name*** For more information about the email address, see **Why Was the Email Address Format Changed in the SOA Record?**	HOSTMASTER@example.com

Parameter	Description	Example Value
Enterprise Project	Enterprise project associated with the public zone. You can manage public zones by enterprise project. **NOTE** This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**. When setting this parameter, note the following: ● If you do not manage zones by enterprise project, select the **default** enterprise project. ● If you manage zones by enterprise project, select an existing enterprise project.	default
Description	(Optional) Supplementary information about the zone. You can enter a maximum of 255 characters.	This is a zone example.

6. Click **OK**.

    You can view the created public zone on the **Public Zones** page.

7. Click the domain name or click **Manage Record Set** under **Operation**.

    On the **Record Sets** page, click **Add Record Set**. For detailed operations, see **Record Set Overview**.

    📖 NOTE

    Click the domain name to view SOA and NS record sets automatically generated for the zone.

    ● The SOA record set identifies the base DNS information about the domain name.
    ● The NS record set defines authoritative DNS servers for the domain name.

Follow-up Operations

After a public zone is created, you can perform the following operations:

● Add record sets for it. For details, see **Record Set Overview**.
● Modify or delete it, or view its details. For details, see **Managing Public Zones**.

3.3 Managing Public Zones

Scenarios

You can modify a public zone, delete a public zone, batch delete public zones, or view details about a public zone.

Modifying a Public Zone

Change the domain name administrator's email address and description of the public zone.

📖 **NOTE**

> For more information about the email, see **Why Was the Email Address Format Changed in the SOA Record?**

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Public Zones**.

   The **Public Zones** page is displayed.

4. Locate the public zone you want to modify and choose **More** > **Modify** under **Operation**.

   The **Modify Public Zone** dialog box is displayed.

5. Change the email address or description of the zone as required.

6. Click **OK**.

Deleting a Public Zone

Delete a public zone when you no longer need it. After a public zone is deleted, the domain name and its subdomains cannot be resolved by the DNS service.

NOTICE

Before you delete a public zone, back up all its record sets.

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Public Zones**.

   The **Public Zones** page is displayed.

4. Locate the public zone you want to delete and click **Delete** under **Operation**.

   The **Delete Public Zone** dialog box is displayed.

5. Click **Yes**.

Viewing Details About a Public Zone

View details about a public zone, such as zone ID, operation time, and TTL, on the **Public Zones** page.

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.
3. On the **Dashboard** page, click **Public Zones** under **My Resources**.
4. In the public zone list, click the name of the public zone to view its details.

4 Private Zones

4.1 Overview

A private zone contains information about how to map a domain name and its subdomains used within one or more VPCs to private IP addresses. With private domain names, your ECSs can communicate with each other within the VPCs without having to connect to the Internet.

- You can create any domain names without registering them.
- One private zone can be associated with multiple VPCs, and domain names are valid only in VPCs.

To use private domain names, you must first create a private zone and associate VPCs with it.

Table 4-1 describes the operations that you can perform on private zones.

Table 4-1 Private zone operations

Operation	Scenario	Constraints
Creating a Private Zone	Create a private zone for your domain name.	- Private zones are project-level resources. When you create a private zone, select a region and project. - Each account can create up to 50 private zones. - Private domain names must meet the following requirements: - Domain name labels are separated by dot (.), and each label does not exceed 63 characters. - A domain name label can contain letters, digits, and hyphens (-) and cannot start or end with a hyphen. - The total length of a domain name cannot exceed 254 characters.
Managing Private Zones	Modify, delete, and view private zones.	- The domain name of a created private zone cannot be modified. - If a private zone is deleted, all its record sets will also be deleted.
Associating a VPC with a Private Zone	Associate a VPC with a private zone.	- You can only associate VPCs that you have created using your own account. - Each VPC can be associated only with one private zone. However, a private zone can have more than one VPC associated with it.
Disassociating a VPC from a Private Zone	Disassociate a VPC from a private zone.	- After the disassociation, private domain names will not take effect in the VPC. - If a private zone is only associated with one VPC, you cannot disassociate it.

4.2 Creating a Private Zone

Scenarios

Create a private zone to map a private domain name to a private IP address within a VPC.

Prerequisites

- You have created a VPC.
- You have created an ECS in the VPC and planned to use a private domain name (example.com) for the ECS.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Private Zones**.

   The **Private Zones** page is displayed.

4. Click ⊙ in the upper left corner and select the desired region and project.

5. Click **Create Private Zone**.

6. Configure the parameters.

   Table 4-2 describes the parameters.

Table 4-2 Parameters for creating a private zone

Parameter	Description	Example Value
Domain Name	Domain name you have planned for the ECS. You can enter a top-level domain that complies with the domain naming rules.	example.com
VPC	VPC to be associated with the private zone. **NOTE** This VPC must be the same as the VPC where your other cloud resources are deployed. If the VPC is different, the domain name cannot be resolved.	N/A
Email	(Optional) Email address of the administrator managing the private zone. Recommended email address: **HOSTMASTER@***Domain name* For more information about the email, see **Why Was the Email Address Format Changed in the SOA Record?**	HOSTMASTER@example.com

Parameter	Description	Example Value
Enterprise Project	Enterprise project associated with the private zone. You can manage private zones by enterprise project. **NOTE** This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**. When setting this parameter, note the following: ● If you do not manage zones by enterprise project, select the **default** enterprise project. ● If you manage zones by enterprise project, select an existing enterprise project.	default
Description	(Optional) Supplementary information about the zone. You can enter a maximum of 255 characters.	This is a zone example.

7. Click **OK**.

8. Switch back to the **Private Zones** page.

   You can view the created private zone in the zone list.

9. Click the domain name to add a record set.

   On the **Record Sets** page, click **Manage Record Set**. For detailed operations, see **Record Set Overview**.

   📖 **NOTE**

   Click the domain name to view SOA and NS record sets automatically generated for the zone.
   ● The SOA record set identifies the base DNS information about the domain name.
   ● The NS record set defines authoritative DNS servers for the domain name.

Follow-up Operations

After a private zone is created, you can perform the following operations:

● Add record sets for it. For details, see **Record Set Overview**.
● Modify or delete it, or view its details. For details, see **Managing Private Zones**.

4.3 Managing Private Zones

Scenarios

You can modify a private zone, delete a private zone, batch delete private zones, or view details about a private zone.

Modifying a Private Zone

Change the domain name administrator's email address and description of the private zone.

📖 **NOTE**

For more information about the email, see **Why Was the Email Address Format Changed in the SOA Record?**

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.

   The **Private Zones** page is displayed.
4. Click 📍 in the upper left corner and select the desired region and project.
5. Locate the private zone you want to modify and choose **More** > **Modify** under **Operation**.

   The **Modify Private Zone** dialog box is displayed.
6. Change the email address or description of the zone as required.
7. Click **OK**.

Deleting a Private Zone

Delete a private zone when you no longer need it. After a private zone is deleted, the domain name and its subdomains cannot be resolved by the DNS service.

NOTICE

Before you delete a private zone, back up all record sets in the private zone.

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.

   The **Private Zones** page is displayed.
4. Click 📍 in the upper left corner and select the desired region and project.

5. Locate the private zone you want to delete and choose **More** > **Delete** in the **Operation** column

6. Click **Yes**.

Viewing Details About a Private Zone

View details about a private zone, such as zone ID, operation time, and TTL, on the **Private Zones** page.

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. On the **Dashboard** page, click **Private Zones** under **My Resources**.

4. Click   in the upper left corner and select the desired region and project.

5. In the private zone list, click the name of the private zone to view its details.

4.4 Associating a VPC with a Private Zone

Scenarios

Associate a VPC with a private zone so that the private domain name can be resolved within this VPC.

☐ NOTE

This VPC must be the same as the VPC where your other cloud resources are deployed. If the VPC is different, the domain name cannot be resolved.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Private Zones**.

   The **Private Zones** page is displayed.

4. Click   in the upper left corner and select the desired region and project.

5. Locate the private zone with which you want to associate the VPC and click **Associate VPC** under **Operation**.

6. Select the VPC you want to associate.

   If no VPCs are available, create one on the VPC console and then associate the private zone with it.

7. Click **OK**.

   The VPC is displayed under **Associated VPC**.

4.5 Disassociating a VPC from a Private Zone

Scenarios

Disassociate a VPC from a private zone if you do not want the private domain name to be resolved in this VPC. If a private zone has only one VPC associated, you cannot disassociate the VPC.

📖 **NOTE**

> If you do not intend to use private domain names, delete the private zone configured for it.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click 📍 in the upper left corner and select the desired region and project.
5. Locate the private zone from which a VPC is to be disassociated, select the VPC to be disassociated under **Associated VPC**, and click ⊗ on the right of the VPC.
6. In the **Disassociate VPC** dialog box, click **Yes**.

5 Record Sets

5.1 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.

Table 5-1 Record set management

Operation	Scenario	Constraints
Adding Record Sets	View record set types supported by the DNS service and their configuration rules. Add record sets to a domain name. For details, see **Table 5-2**.	● After a zone is created for a domain name, the system automatically creates the SOA and NS record sets. ● A maximum of 500 record sets can be added in an account.
Managing Record Sets	Modify, delete, and view record sets.	● After a record set is added, its resolution line cannot be modified. ● You cannot modify or delete SOA and NS record sets automatically generated by the system.
Configuring a Wildcard DNS Record Set	Add a record set that matches all subdomains.	Wildcard DNS resolution does not support NS and SOA record sets.

Figure 5-1 shows the process for configuring a record set on the DNS console.

Figure 5-1 Process for configuring a record set
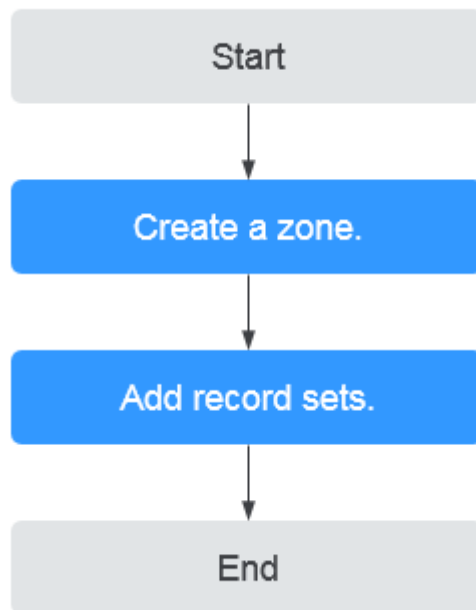
☐ **NOTE**

Either a public or private zone can be created. For details, see the following:

- **Creating a Public Zone**
- **Creating a Private Zone**

5.2 Adding Record Sets

5.2.1 Record Set Types and Configuration Rules

Record Set Types

Table 5-2 describes the record set types.

- Record set types in public zones: A, CNAME, MX, AAAA, TXT, SRV, NS, SOA, and CAA
- Record set types in private zones: A, CNAME, MX, AAAA, TXT, SRV, SOA, and PTR

Table 5-2 Record set types

Record Set Type	Description	Value	Example
A	Maps domains to IPv4 addresses.	IPv4 addresses mapped to the domain name You can enter a maximum of 50 record values, each on a separate line.	192.168.12.2 192.168.12.3
CNAME	Maps one domain name to another domain name or multiple domain names to one domain name.	Domain name alias. You can enter only one domain name.	www.example.com
MX	Maps domain names to email servers.	Email server address You can enter a maximum of 50 record values, each on a separate line. The format is **[priority][mail server host name]**. Configuration rules: ● **priority**: priority for an email server to receive emails. A smaller value indicates a higher priority. ● **mail server host name**: domain name provided by the email service provider	10 mailserver.example.com. 20 mailserver2.example.com.

Record Set Type	Description	Value	Example
AAAA	Maps domain names to IPv6 addresses.	IPv6 addresses mapped to the domain name You can enter a maximum of 50 record values, each on a separate line.	ff03:0db8:85a3:0:0:8 a2e:0370:7334

Record Set Type	Description	Value	Example
TXT	Creates text records for domain names. It is usually used in the following scenarios: ● To record DKIM public keys to prevent email fraud. ● To record the identity of domain name owners to facilitate domain name retrieval.	Text content Configuration rules: ● Text record values must be enclosed in double quotation marks. ● One or more text record values are supported, each on a separate line. A maximum of 50 text record values can be entered. ● A single text record value can contain multiple character strings, each of which is double quoted and separated from others using a space. One character string cannot exceed 255 characters. A value must not exceed 4096 characters. ● The value cannot be left blank. ● The text cannot contain a backslash (\).	● Single text record: "aaa" ● Multiple text records: "bbb" "ccc" ● A text record that contains multiple strings: "ddd" "eee" "fff"

Record Set Type	Description	Value	Example
SRV	Records servers providing specific services.	Server address You can enter a maximum of 50 record values, each on a separate line. The value format is **[priority] [weight] [port number] [server address]**. Configuration rules: • The priority, weight, and port number range from 0 to 65535. • A smaller value indicates a higher priority. • A larger value indicates a larger weight. • The server address is the domain name of the target server. Ensure that the domain name can be resolved. **NOTE** If the record set values have the same priority, requests to the domain name will be routed based on weights.	2 1 2355 example_server.test.com

Record Set Type	Description	Value	Example
NS	Delegates subdomains to other name servers. ● For public zones, an NS record set is automatically created, and you can add NS record sets for subdomains. ● For private zones, an NS record set is automatically created, and you cannot add other NS record sets.	DNS server address You can enter a maximum of 50 record values, each on a separate line.	ns1.example.net ns2.example.net
SOA	Identifies the base information about a domain name. The SOA record set is automatically generated by the DNS service and cannot be added manually.	This type of record set is created by default and cannot be added manually.	This type of record set is created by default and cannot be added manually.

Record Set Type	Description	Value	Example

CAA	Grants certificate issuing permissions to certificate authorities (CAs). CAA record sets can prevent the issuance of unauthorized HTTPS certificates.	CA to be authorized to issue certificates for a domain name or its subdomains
		
		You can enter a maximum of 50 record values, each on a separate line.
		
		The format is **[flag] [tag] [value]**.
		
		Configuration rules:
		
		• **flag**: CA identifier, an unsigned character ranging from 0 to 255. Usually, the value is set to **0**.
		
		• **tag**: You can enter 1 to 15 characters, consisting of letters and digits from 0 to 9. The tag can be one of the following:
		
		  – **issue**: authorizes a CA to issue all types of certificates.
		
		  – **issuewild**: authorizes a CA to issue wildcard certificates.
		
		  – **iodef**: requests notifications
			0 issue "ca.abc.com"
			
			0 issuewild "ca.def.com"
			
			0 iodef "mailto:admin@domain.com"
			
			0 iodef "http://domain.com/log/"

Record Set Type	Description	Value	Example
		once a CA receives invalid certificate requests. • **value**: authorized CA or email address/URL required for notification once the CA receives invalid certificate requests. The value depends on the value of **tag** and must be enclosed in quotation marks (""). The value can contain a maximum of 255 characters, consisting of letters, digits, spaces, and special characters -#*?&_~=:;.@+^/!%	
PTR	Maps IP addresses to domain names.	Private domain name mapped to the private IP address. You can enter only one domain name.	www.example.com

5.2.2 Adding an A Record Set

Scenarios

If you want end users to access your website, web application, or cloud server configured with an IPv4 address via its domain name, add an A record set for this domain name.

For more information about the types of record sets, see **Record Set Types and Configuration Rules**.

Prerequisites

You have a website, web application, or cloud server and obtained an IPv4 address.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane, choose **Public Zones** or **Private Zones**.

   The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click 📍 on the upper left corner to select the region and project.

5. Click the domain name.

6. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.

7. Configure the parameters based on **Table 5-3**.

Table 5-3 Parameters for adding an A record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved. For example, if the domain name is **example.com**, the prefix can be as follows: ● **www**: The domain name is www.example.com, which is usually used for a website. ● Left blank: The domain name is example.com. The **Name** field cannot be set to an at sign (@). Just leave it blank. ● **abc**: The domain name is abc.example.com, a subdomain of example.com. ● **mail**: The domain name is mail.example.com, which is typically used for email servers. ● *****: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com.	www

Parameter	Description	Example Value
Type	Type of the record set. A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set.	A – Map domains to IPv4 addresses
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300
Value	IPv4 addresses mapped to the domain name. You can enter a maximum of 50 record values, each on a separate line.	192.168.12.2 192.168.12.3
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only designated for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1
Description	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	N/A

Table 5-4 Tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 characters. ● Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Cannot start or end with a space nor contain special characters =*<>\,|/	example_value1

8. Click **OK**.

9. Switch back to the **Record Sets** tab.

   You can view the added record set in the **Normal** state.

Related Operations

For details about how to configure A record sets, see **Routing Internet Traffic to a Website**.

5.2.3 Adding a CNAME Record Set

Scenarios

If you want to map one domain name to another, add a CNAME record set for the domain name.

For more details, see **Record Set Types and Configuration Rules**.

Constraints

- You can leave the **Name** parameter blank when adding a CNAME record set.
- You cannot create a CNAME record set with the same name and resolution line as an NS record set.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane, choose **Public Zones** or **Private Zones**.

   The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click   on the upper left corner to select the region and project.

5. Click the domain name.

6. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.

7. Configure the parameters based on **Table 5-5**.

Table 5-5 Parameters for adding a CNAME record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved. For example, if the domain name is **example.com**, the prefix can be as follows: ● **www**: The domain name is www.example.com, which is usually used for a website. ● Left blank: The domain name is example.com. The **Name** field cannot be set to an at sign (@). Just leave it blank. ● **abc**: The domain name is abc.example.com, a subdomain of example.com. ● **mail**: The domain name is mail.example.com, which is typically used for email servers. ● *****: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com.	Left blank
Type	Type of the record set A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set.	CNAME – Map one domain to another
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300
Value	Domain name alias. You can enter only one domain name.	webserver01.example.com
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only designated for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1

Parameter	Description	Example Value
Descriptio n	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	-

8. Click **OK**.
9. Switch back to the **Record Sets** tab.

   You can view the added record set in the **Normal** state.

5.2.4 Adding an MX Record Set

Scenarios

If you want to map email servers to a domain name, you can add MX record sets.

For details about other types of record sets, see **Record Set Types and Configuration Rules**.

Prerequisites

You have deployed an email server and obtained its domain name.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.
3. In the navigation pane, choose **Public Zones** or **Private Zones**.

   The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click ⊙ on the upper left corner to select the region and project.
5. Click the domain name.
6. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
7. Configure the parameters based on **Table 5-6**.

Table 5-6 Parameters for adding an MX record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved. For example, if the domain name is **example.com**, the prefix can be as follows: ● **www**: The domain name is www.example.com, which is usually used for a website. ● Left blank: The domain name is example.com. The **Name** field cannot be set to an at sign (@). Just leave it blank. ● **abc**: The domain name is abc.example.com, a subdomain of example.com. ● **mail**: The domain name is mail.example.com, which is typically used for email servers. ● *****: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com.	Left blank
Type	Type of the record set A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set.	MX – Map domains to email servers
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300
Value	Email server address You can enter a maximum of 50 record values, each on a separate line. The format is **[priority][mail server host name]**. Configuration rules: ● **priority**: priority for an email server to receive emails. A smaller value indicates a higher priority. ● **mail server host name**: domain name provided by the email service provider	10 mailserver.example.com.

Paramete r	Description	Example Value
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only designated for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1
Descriptio n	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	-

8. Click **OK**.

9. Switch back to the **Record Sets** tab.

   You can view the added record set in the **Normal** state.

5.2.5 Adding an AAAA Record Set

Scenarios

If you want end users to access your website, web application, or cloud server configured with an IPv6 address via its domain name, add an AAAA record set for this domain name.

For more details, see **Record Set Types and Configuration Rules**.

Prerequisites

You have a web server and obtained an IPv6 address.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane, choose **Public Zones** or **Private Zones**.

   The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click   on the upper left corner to select the region and project.

5. Click the domain name.

6. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.

7. Configure the parameters based on **Table 5-7**.

Table 5-7 Parameters for adding an AAAA record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved. For example, if the domain name is **example.com**, the prefix can be as follows: ● **www**: The domain name is www.example.com, which is usually used for a website. ● Left blank: The domain name is example.com. The **Name** field cannot be set to an at sign (@). Just leave it blank. ● **abc**: The domain name is abc.example.com, a subdomain of example.com. ● **mail**: The domain name is mail.example.com, which is typically used for email servers. ● *****: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com.	www
Type	Type of the record set. A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set.	AAAA – Map domains to IPv6 addresses
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300
Value	IPv6 addresses mapped to the domain name You can enter a maximum of 50 record values, each on a separate line.	ff03:0db8:85a 3:0:0:8a2e:037 0:7334

Parameter	Description	Example Value
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only designated for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1
Description	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	-

8. Click **OK**.

9. Switch back to the **Record Sets** tab.

   You can view the added record set in the **Normal** state.

5.2.6 Adding a TXT Record Set

Scenarios

A TXT record set provides description for a domain name.

For details about other record set types, see **Record Set Types and Configuration Rules**.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane, choose **Public Zones** or **Private Zones**.

   The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click ⊙ on the upper left corner to select the region and project.

5. Click the domain name.

6. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.

7. Configure the parameters based on **Table 5-8**.

Table 5-8 Parameters for adding a TXT record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved. For example, if the domain name is **example.com**, the prefix can be as follows: ● **www**: The domain name is www.example.com, which is usually used for a website. ● Left blank: The domain name is example.com. The **Name** field cannot be set to an at sign (@). Just leave it blank. ● **abc**: The domain name is abc.example.com, a subdomain of example.com. ● **mail**: The domain name is mail.example.com, which is typically used for email servers. ● *****: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com.	Left blank
Type	Type of the record set A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set.	TXT – Specify text records
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300

Parameter	Description	Example Value
Value	Text content Configuration rules: • Text record values must be enclosed in double quotation marks. • One or more text record values are supported, each on a separate line. A maximum of 50 text record values can be entered. • A single text record value can contain multiple character strings, each of which is double quoted and separated from others using a space. One character string cannot exceed 255 characters. A value must not exceed 4096 characters. • The value cannot be left blank. • The text cannot contain a backslash (\).	• Single text record: "aaa" • Multiple text records: "bbb" "ccc" • A text record that contains multiple strings: "ddd" "eee" "fff"
Description	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	-

8. Click **OK**.

9. Switch back to the **Record Sets** tab.

   You can view the added record set in the **Normal** state.

5.2.7 Adding an SRV Record Set

Scenarios

To tag a server to show what services it provides, you can add SRV record sets for a domain name.

For details about other record set types, see **Record Set Types and Configuration Rules**.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane, choose **Public Zones** or **Private Zones**.

   The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click ⊙ on the upper left corner to select the region and project.

5. Click the domain name.

6. Click **Add Record Set**.

    The **Add Record Set** dialog box is displayed.

7. Configure the parameters based on **Table 5-9**.

Table 5-9 Parameters for adding an SRV record set

Parameter	Description	Example Value
Name	Service (for example, FTP, SSH, or SIP) provided over the specified protocol (for example, TCP or UDP) on a host The format is _Service name._Protocol.	_ftp._tcp **_ftp._tcp** indicates that the host provides the FTP service over TCP.
Type	Type of the record set A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set.	SRV – Record servers providing specific services
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300

Value	Server address
	
	You can enter a maximum of 50 record values, each on a separate line.
	
	The value format is **[priority] [weight] [port number] [server address]**.
	
	Configuration rules:
	
	● The priority, weight, and port number range from 0 to 65535.
	
	● A smaller value indicates a higher priority.
	
	● A larger value indicates a larger weight.
	
	● The server address is the domain name of the target server.
	  Ensure that the domain name can be resolved.
	
	NOTE
	  If the record set values have the same priority, requests to the domain name will be routed based on weights.
		2 1 2355 example_server.test.com

Paramete r	Description	Example Value
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only designated for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1
Descriptio n	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	-

8. Click **OK**.

9. Switch back to the **Record Sets** tab.

   You can view the added record set in the **Normal** state.

5.2.8 Adding an NS Record Set

Scenarios

If you want to specify authoritative DNS servers for a domain name, you can add NS record sets.

For more details, see **Record Set Types and Configuration Rules**.

Constraints

- You can create NS record sets only in public zones.

- After a public zone is created, an NS record set is automatically created for this zone and cannot be deleted. You can add NS record sets only in the following scenarios:

  - The **Name** parameter is not left blank. This means that you can add NS record sets for subdomains of a domain name.

  - The value of the **Line** parameter is not set to **Default**. This means that you can add NS record sets for the domain name with other resolution lines.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Public Zones**.

   The **Public Zones** page is displayed.

4. Click the domain name.

5. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.

6. Configure the parameters based on **Table 5-10**.

Table 5-10 Parameters for adding an NS record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved. For example, if the domain name is **example.com**, the prefix can be as follows: • **www**: The domain name is www.example.com, which is usually used for a website. • Left blank: The domain name is example.com. The **Name** field cannot be set to an at sign (@). Just leave it blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com, which is typically used for email servers. • *****: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com.	abc
Type	Type of the record set A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set.	NS – Delegate subdomains to other name servers
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300
Value	DNS server address You can enter a maximum of 50 record values, each on a separate line.	ns1.example.net ns2.example.net

Parameter	Description	Example Value
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only designated for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1
Description	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	-

7. Switch back to the **Record Sets** tab.

   You can view the added record set in the **Normal** state.

5.2.9 Adding a CAA Record Set

Scenarios

If you want to specify CAs authorized to issue HTTPS certificates for your domain name, add CAA record sets for the domain name.

CAA record sets are used to prevent HTTPS certificates from being incorrectly issued.

For details about other record set types, see **Record Set Types and Configuration Rules**.

Constraints

CAA record sets can be added only to public zones.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Public Zones**.

   The **Public Zones** page is displayed.

4. Click the domain name.

5. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.

6. Configure the parameters based on **Table 5-11**.

Table 5-11 Parameters for adding a CAA record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved. For example, if the domain name is **example.com**, the prefix can be as follows: ● **www**: The domain name is www.example.com, which is usually used for a website. ● Left blank: The domain name is example.com. The **Name** field cannot be set to an at sign (@). Just leave it blank. ● **abc**: The domain name is abc.example.com, a subdomain of example.com. ● **mail**: The domain name is mail.example.com, which is typically used for email servers. ● *****: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com.	Left blank
Type	Type of the record set A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set.	CAA – Grant certificate issuing permissions to CAs
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300

Parameter	Description	Example Value
Value	CA to be authorized to issue certificates for a domain name or its subdomains You can enter a maximum of 50 record values, each on a separate line. The format is **[flag] [tag] [value]**. Configuration rules: ● **flag**: CA identifier, an unsigned character ranging from 0 to 255. Usually, the value is set to **0**. ● **tag**: You can enter 1 to 15 characters, consisting of letters and digits from 0 to 9. The tag can be one of the following: – **issue**: authorizes a CA to issue all types of certificates. – **issuewild**: authorizes a CA to issue wildcard certificates. – **iodef**: requests notifications once a CA receives invalid certificate requests. ● **value**: authorized CA or email address/URL required for notification once the CA receives invalid certificate requests. The value depends on the value of **tag** and must be enclosed in quotation marks (""). The value can contain a maximum of 255 characters, consisting of letters, digits, spaces, and special characters -#*?&_~=:;.@+^/!%	0 issue "ca.abc.com" 0 issuewild "ca.def.com" 0 iodef "mailto:admin@domain.com" 0 iodef "http://domain.com/log/"
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only designated for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1
Description	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	-

7. Switch back to the **Record Sets** tab.

   You can view the added record set in the **Normal** state.

5.2.10 Adding a PTR Record Set

Scenarios

You can create PTR record sets to map private IP addresses to domain names.

For details about other record set types, see **Record Set Types and Configuration Rules**.

Constraints

- You can create PTR record sets only in private zones.
- PTR record sets can only be added to private zones whose domain name suffix is in-addr.arpa.

  For details about how to create a PTR record for a public domain name, see **Creating a PTR Record**.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.

   The **Private Zones** page is displayed.
4. Click ⦿ in the upper left corner and select the desired region and project.
5. Click the domain name.
6. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
7. Configure the parameters based on **Table 5-12**.

Table 5-12 Parameters for adding a PTR record set

Parameter	Description	Example Value
Name	Name of the PTR record set	10.1.168 For example, if the IP address is 192.168.1.10, the domain name in the PTR record is **10.1.168.192.in-addr.arpa**. ● If the private zone is 192.in-addr.arpa, enter **10.1.168** in the box. ● If the private zone is 1.168.192.in-addr.arpa, enter **10** in the box.
Type	Type of the record set A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set.	PTR – Map IP addresses to domains
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300
Value	Private domain name mapped to the private IP address. You can enter only one domain name.	host.example.com.
Description	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	-

8. Click **OK**.
9. Switch back to the **Record Sets** tab.

    You can view the added record set in the **Normal** state.

Related Operations

For more information, see **How Can I Map the Private IP Address of an ECS to a Domain Name?**

5.3 Managing Record Sets

Scenarios

You can modify or delete record sets, and view their details.

Modifying a Record Set

Change the TTL, value, and description of a record set to better address your service requirements.

📖 NOTE

SOA and NS record sets are automatically generated and cannot be modified.

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane, choose **Public Zones** or **Private Zones**.

   The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click 📍 on the upper left corner to select the region and project.

5. Click the domain name.

   The **Record Sets** page is displayed.

6. Locate the record set you want to modify and click **Modify** under **Operation**.

   The **Modify Record Set** dialog box is displayed.

7. Modify the parameters.

   You can change only the TTL, value, and description of a record set.

8. Click **OK**.

Deleting a Record Set

📖 NOTE

SOA and NS record sets are automatically generated and cannot be deleted.

Record sets that are no longer required can be deleted. After a record set is deleted, it will become unavailable. For example, if an A record set is deleted, the domain name cannot be resolved into the IPv4 address specified in the record set. If a CNAME record set is deleted, the domain alias cannot be mapped to the domain name.

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. On the **Dashboard** page, click **Public Zones** or **Private Zones**.

   The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click on the upper left corner to select the region and project.

5. Click the domain name.

    The **Record Sets** page is displayed.

6. Locate the record set you want to delete and click **Delete** under **Operation**.

7. In the **Delete Record Set** dialog box, click **Yes**.

Viewing Details About a Record Set

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

    The DNS console is displayed.

3. In the navigation pane, choose **Public Zones** or **Private Zones**.

    The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click on the upper left corner to select the region and project.

5. Click the domain name.

    The **Record Sets** page is displayed.

6. Locate the record set you want to view and click its name to view the details.

5.4 Configuring a Wildcard DNS Record Set

Scenarios

A wildcard record set with its name set to an asterisk (*) can map all subdomains of the domain name to the same value. During domain name resolution, fuzzy match is used.

📖 **NOTE**

Exact match has a higher priority than fuzzy match.

Constraints

Wildcard DNS resolution does not support NS and SOA record sets.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

    The DNS console is displayed.

3. In the navigation pane, choose **Public Zones** or **Private Zones**.

    The zone list is displayed.

4. (Optional) If you have selected **Private Zones**, click on the upper left corner to select the region and project.

5. Click the name of the zone to which you want to add a wildcard DNS record set.

6. Click **Add Record Set**.

7. Configure the parameters based on **Table 5-13**.

Table 5-13 Parameters for adding a wildcard DNS record set

Parameter	Description	Example Value
Name	Public (or private) domain name Enter an asterisk (*) as the leftmost label of the domain name, for example, ***.example.com**. NOTE Only the leftmost asterisk is considered as a wildcard character. Other asterisks in the domain name are common text characters.	*.abc
Type	Record set type Wildcard DNS resolution does not support NS and SOA record sets.	A – Map domains to IPv4 addresses
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	300
Value	Record set value	Take an A record set for example, **Value** is set to IPv4 addresses mapped to the domain name. Example: 192.168.12.2 192.168.12.3
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only designated for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1

Paramete r	Description	Example Value
Descriptio n	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	This is a wildcard DNS record set.

8. Click **OK**.
9. Switch back to the **Record Sets** tab.

   You can view the wildcard DNS record set in the **Normal** state.

6 PTR Records

6.1 Overview

Reverse resolution means to obtain a domain name based on an IP address. 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 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. Therefore, it is necessary to map IP addresses of your email servers to domain names by adding PTR records.

Table 6-1 PTR record description

Operation	Scenario	Constraints
Creating a PTR Record	Create PTR records for cloud resources such as ECS.	- PTR records are project-level resources. When you create a PTR record, you need to select a region and project. - Each user can add a maximum of 50 PTR records.
Managing PTR Records	Modify, delete, and query PTR records.	- After you created a PTR record, its EIP cannot be changed. - After you delete a PTR record, the domain name mapped to your EIP will change to the default domain name.

6.2 Creating a PTR Record

Scenarios

PTR records are used to prove credibility of IP addresses and domain names of email servers. To avoid being tracked, most spam senders use email servers whose IP addresses are dynamically allocated or not mapped to registered domain names. If you want to keep the spam out of your recipients' inbox, add a PTR record to map the email server IP address to a domain name. In this way, the email recipients can obtain the domain name by IP address and will know that the email server is trustworthy.

If you use an ECS as an email server, configure a PTR record to map the EIP of the ECS to the domain name.

This following are operations for you to add a PTR record for a cloud resource, such as ECS.

Constraints

You can only configure PTR records for IP addresses with a 32-bit subnet mask.

Prerequisites

- You have registered a domain name.
- You have created an ECS and bound an EIP to it.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **PTR Records**.
   The **PTR Records** page is displayed.
4. Click ⦿ in the upper left corner and select the desired region and project.
5. Click **Create PTR Record**.
6. Configure the parameters based on **Table 6-2**.

Table 6-2 Parameters for creating a PTR record

Parameter	Description	Example Value
EIP	EIP of another cloud resource, for example, ECS. You can select an EIP from the drop-down list.	XX.XX.XX.XX

Parameter	Description	Example Value
Domain Name	Domain name mapped to the EIP.	example.com
TTL (s)	Cache duration of the PTR record, in seconds The default value is 300s.	300
Enterprise Project	Enterprise project associated with the PTR record. You can manage PTR records by enterprise project. **NOTE** This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**. When setting this parameter, note the following: ● If you do not manage PTR records by enterprise project, select the **default** enterprise project. ● If you manage PTR records by enterprise project, select an existing enterprise project.	default
Description	(Optional) Supplementary information about the PTR record.	The description of the PTR record

7. Click **OK**.

   You can view the created PTR record on the **PTR Records** page.

   ◻ **NOTE**

   If a domain name is mapped to multiple EIPs, you must create a PTR record for each EIP.

8. Verify that the PTR record has taken effect by running the following command on a PC connected to the Internet:

   nslookup -qt=ptr *EIP*

6.3 Managing PTR Records

Scenarios

You can modify a PTR record, delete a PTR record, batch delete PTR records, or view details about a PTR record.

Modifying a PTR Record

Modify the domain name, TTL, or description of a PTR record.

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

    The DNS console is displayed.
3. In the navigation pane on the left, choose **PTR Records**.

    The **PTR Records** page is displayed.
4. Click ⊙ in the upper left corner and select the desired region and project.
5. Locate the PTR record you want to modify and click **Modify** under **Operation**.

    The **Modify PTR Record** dialog box is displayed.
6. Change the domain name, TTL, or description as required.
7. Click **OK**.

Deleting a PTR Record

Delete a PTR record if you no longer need it. After you delete a PTR record, the domain name mapped to your EIP will change to the default domain name.

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

    The DNS console is displayed.
3. In the navigation pane on the left, choose **PTR Records**.

    The **PTR Records** page is displayed.
4. Click ⊙ in the upper left corner and select the desired region and project.
5. Locate the PTR record you want to delete and click **Delete** under **Operation**.
6. Click **Yes**.

Viewing Details About a PTR Record

After a PTR record is created, you can view its details, including the zone ID, TTL, and EIP.

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

    The DNS console is displayed.
3. In the navigation pane on the left, choose **PTR Records**.

    The **PTR Records** page is displayed.
4. Click ⊙ in the upper left corner and select the desired region and project.
5. In the PTR record list, view the record details.

7 Intelligent Resolution

7.1 Configuring Weighted Routing

Scenarios

A large website is generally deployed on multiple servers. To balance the load of each server, you can use weights to control the proportion of requests to each server.

The DNS service allows you to set weights to record sets to route the requests to different servers based on the specified weights.

When your website has multiple servers and each server has an independent IP address, consider weighted routing to distribute requests to different servers proportionally.

For example, you have a website deployed on three servers. The domain name of your website is example.com, and the IP addresses of the three servers are 192.168.1.1, 192.168.1.2, and 192.168.1.3.

- If you add an A record set and set its value to the three IP addresses, with no weights set to the IP addresses, requests are randomly routed to an IP address.

  For details, see

- You add three A record sets, with each having an IP address as its value.

  In this case, you can set different weights for the three record sets. In this way, requests are routed to each server based on the specified weight.

Weighted routing can better distribute requests and balance server load. You can perform the operations provided in this section to set the weights.

Constraints

You can configure weights for up to 20 record sets of the same domain name and line.

Preparations

There are three web servers. Three A record sets are required, with the value of each set to the IP address of a web server. You can set different weights to control the proportion of requests to each server.

Table 7-1 Weight setting plans

Plan	Domain Name	Record Set Type	Line Type	Value	Weight	Description
1	example.com	A	Default	192.168.1.1	1	Requests are evenly distributed to three servers (the proportion of requests is 1:1:1).
				192.168.1.2	1	
				192.168.1.3	1	
2	example.com	A	Default	192.168.1.1	2	Requests are distributed to three servers in a proportion of 2:3:1. For example, if there are six requests, two are routed to the server whose IP address is 192.168.1.1, three are routed to the server whose IP address is 192.168.1.2, and one is routed to the server whose IP address is 192.168.1.3.
				192.168.1.2	3	
				192.168.1.3	1	

Prerequisites

The domain name of the website has been hosted on the DNS service.

Procedure

The following describes how to add three A record sets to domain name example.com, and the weight ratio of the three record sets is 1:1:1.

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Public Zones**.

   The **Public Zones** page is displayed.

4. On the **Public Zones** page, click the domain name (**example.com**) of the public zone.

The **Record Sets** page is displayed.

5. Click **Add Record Set**.

Figure 7-1 Setting weights

6. Configure the parameters as follows:
   – **Name**: Leave this parameter blank. The DNS service automatically considers example.com as the name, and requests are routed to example.com.
   – **Type**: Set it to **A – Map domains to IPv4 addresses**.
   – **Line Type**: Select **Default**.
   – **Value**: Set it to **192.168.1.1**, the IP address of a web server.
   – **Weight**: Set it to **1**.
7. Click **OK**.
8. Repeat **5** to **7** to add the second and third record sets.
   Set the record set value to 192.168.1.2 and 192.168.1.3, respectively.
   Requests will be evenly distributed to the three servers.

8 Permissions Management

8.1 Creating a User and Granting DNS Permissions

To implement fine-grained permissions control over your DNS resources, **IAM** is a good choice. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing DNS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust another account or cloud service to perform efficient O&M on your DNS resources.

Skip this part if your account does not need individual IAM users.

The following describes the procedure for granting permissions (see **Figure 8-1**).

Prerequisites

You have learned about DNS permissions (see **Permissions**) and have chosen the right policies or roles based on your requirements. For the permission policies of other services, see **System Permissions**.

Process Flow

Figure 8-1 Process for granting permissions
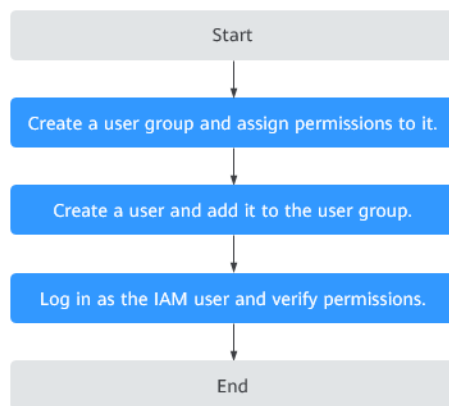
1. **Create a user group and assign permissions**.

   Create a user group on the IAM console and assign the **DNS Administrator** policy to the group.

2. **Create a user and add the user to the user group**

   Create a user on the IAM console and add the user to the group created in step **1**.

3. **Log in to the management console as the created user**.

   Log in to the DNS console by using the created user, and verify that the user only has read permissions for DNS.

   – Choose **Service List** > **Domain Name Service**. On the **Dashboard** page, click **Private Zones**. Then click **Create Private Zone** in the upper right corner. If the private zone can be created, the DNS Administrator policy is in effect.

   – Choose any other service from **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **DNS Administrator** policy is in effect.

9 Key Operations Recorded by CTS

9.1 DNS Operations Recorded by CTS

CTS records DNS operations performed by users in real time. Actions and results of the operations are stored in OBS buckets in the form of traces.

After you enable CTS, whenever a DNS API is called, the operation is recorded in a log file, which is then delivered to a specified OBS bucket for storage.

Table 9-1 and **Table 9-2** list the DNS operations that will be recorded by CTS.

📖 **NOTE**

The DNS service involves resources both at the global and region levels. **Table 9-1** lists DNS operations at the global level. Traces of these operations are displayed only in the primary region.

Table 9-2 lists DNS operations at the region level. Traces of these operations are displayed in the regions where the operations are performed.

Table 9-1 Global-level DNS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a record set for a public zone	publicRecordSet	createPublicRecordSet
Deleting a record set from a public zone	publicRecordSet	deletePublicRecordSet
Modifying a record set of a public zone	publicRecordSet	updatePublicRecordSet
Creating a public zone	publicZone	createPublicZone
Modifying a public zone	publicZone	updatePublicZone
Deleting a public zone	publicZone	deletePublicZone

Table 9-2 Region-level DNS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a record set in a private zone	privateRecordSet	createPrivateRecordSet
Deleting a record set from a private zone	privateRecordSet	deletePrivateRecordSet
Modifying a record set of a private zone	privateRecordSet	updatePrivateRecordSet
Creating a private zone	privateZone	createPrivateZone
Modifying a private zone	privateZone	updatePrivateZone
Deleting a private zone	privateZone	deletePrivateZone
Associating a VPC with a private zone	privateZone	associateRouter
Disassociating a VPC from a private zone	privateZone	disassociateRouter

9.2 Viewing Traces

Scenarios

After CTS is enabled, the tracker starts recording operations on cloud resources. You can view operation records of the last 7 days on the CTS console.

This section describes how to query these records.

Procedure

1. Log in to the management console.

2. Click   in the upper left corner and select the desired region and project.

3. In the service list, choose **Management & Deployment** > **Domain Name Service**.

4. In the navigation pane, choose **Trace List**.

5. Specify the filters used for querying traces. The following filters are available:

   – **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

     Select a filter from the drop-down list.

     If you select **Trace name** for **Search By**, specify a trace name.

     If you select **Resource ID** for **Search By**, specify a resource ID.

     If you select **Resource name** for **Search By**, specify a resource name.

   – **Operator**: Select a user who performs operations.

   – **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.

- Time range: Specify the start and end time to view traces generated during a time range of the last seven days.

6. Click ⌄ on the left of the required trace to expand its details.

7. Click **View Trace**.

A dialog box is displayed, in which the trace structure details are displayed.

10 Quota Adjustment

What Is Quota?

Quotas put limits on the quantities and capacities of resources available to users. Examples of DNS quotas include the maximum number of zones, PTR records, and record sets that you can create. Quotas are put in place to prevent excessive resource usage and ensure service availability for users.

If existing resource quotas cannot meet your service requirements, you can request higher quotas.

How Do I View My Quotas?

1. Log in to the management console.

2. In the upper right corner of the page, click   .
   The **Service Quota** page is displayed.

3. View the used and total quota of each type of resources on the displayed page.
   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

The system does not support online quota adjustment.

If you need to adjust a quota, contact the operations administrator.

11 FAQ

11.1 DNS Overview

11.1.1 Will I Be Billed for the DNS Service?

DNS is a free service.

11.1.2 How Many Zones, PTR Records, and Record Sets Can I Create?

By default, an account to create up to 50 public zones, 50 private zones, 50 PTR records, and 500 record sets.

If the quotas do not meet your service requirements, contact customer service for higher quotas.

11.1.3 What Are DNS Servers?

DNS provides authoritative DNS servers for domain name resolution. The NS record set defines the addresses of authoritative DNS servers for the domain name.

The following are DNS servers:

- ns1.prod-cloud-ocb.orange-business.com
- ns2.prod-cloud-ocb.orange-business.com

For each public zone, an NS record is automatically created, and its value is the two DNS servers.

11.1.4 What Are the Differences Between Public and Private Domain Names?

The most notable difference between public and private domain names is that public domain names are used and must be unique on the Internet, while private domain names are used in VPCs.

To enable a public domain name to be resolved, you need to perform the following steps:

1. Purchase the domain name from a domain name registrar.
2. Create a zone and add records. For details, see **Routing Internet Traffic to a Website**.

For details about how a public domain name is resolved, see **Public Domain Name Resolution**.

Private domain names do not need to be registered and are accessible only in VPCs.

For details about how a private domain name is resolved, see **Routing Traffic Within VPCs**.

11.1.5 Does DNS Support IPv6?

Yes. DNS can translate domain names to both IPv4 and IPv6 addresses.

To translate a domain name to an IPv4 address, add an A record set. To translate a domain name to an IPv6 address, add an AAAA record set.

If your domain name is example.com, you can add the following record sets.

Table 11-1 Record sets

Domain Name	Type	Value
www.example.com	A	192.168.1.2
www.example.com	AAAA	2407:c080:0:ffff:ffff:fffe:0:1

DNS servers (ns1.prod-cloud-ocb.orange-business.com and ns2.prod-cloud-ocb.orange-business.com) support both IPv4 and IPv6 addresses.

Local DNS servers, either supporting IPv4 or IPv6 or both, can send DNS queries to DNS servers.

11.1.6 Does DNS Support Explicit and Implicit URLs?

No.

Explicit or implicit URL forwarding is not performed over a standard DNS protocol, but uses 301 or 302 redirection over HTTP. You can resolve the domain name to the IP address of your cloud server, and then configure 301 or 302 redirection for the domain name on your web server, such as Nginx, Apache, and Internet Information Services (IIS).

11.1.7 Does DNS Support Dynamic Domain Name Resolution?

No. DNS can only translate domain names to fixed IPv4 and IPv6 addresses.

11.1.8 Does DNS Support Wildcard Entries?

Yes. DNS allows you to configure wildcard entries.

A wildcard entry is a record set that uses an asterisk (*) as the name and matches requests for any domain name based on the configuration you set. For more information, see RFC 4592.

DNS supports wildcard entries for the following record set types: A, AAAA, MX, CNAME, TXT, PTR, CAA, and SRV.

11.1.9 What Is TTL?

TTL (time to live) specifies how long records are cached on a local DNS server.

The local DNS server is connected to clients (computers or smartphones) through the Internet. By default, its address is assigned by the broadband carrier. You can also choose a public DNS server as your local DNS server.

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.**Managing Record Sets**.

11.1.10 How Many Domain Name Levels Does DNS Support?

The DNS service supports two levels of public domain names.

DNS supports the following levels for domain names with the .com suffix:

- Primary domain name, such as example.com
- Subdomain, such as www.example.com

DNS supports the following levels for domain names with the .com.cn suffix:

- Primary domain name, such as example.com.cn
- Subdomain, such as www.example.com.cn

11.1.11 How Are Zones Queried to Resolve a Domain Name?

When a domain name resolution request is initiated, a matched subdomain is first queried.

- If a zone is created for the subdomain, the system returns the result based on the zone configuration.
- If a zone is not created for the subdomain, the system queries the domain name in the zone created for the domain name.

For example, suppose you have created one zone for **example.com** and added an A record set with the **Name** field set to **www**. You have also created another zone for **www.example.com** without an A record set.

If an end user accesses www.example.com, the domain name **www.example.com** is first queried. However, no result will be returned because no record sets have been added to the zone.

11.1.12 Why Was the Email Address Format Changed in the SOA Record?

When you add a record set, you can enter an email address to receive error information and problem reports of the domain name. However, based on RFC 2142, we strongly recommend that you use **HOSTMASTER@***Domain name* as the email address.

Because the at sign (@) has a special meaning in the SOA record set, the system replaces it with a dot (.) and includes a backslash (\) before the dot in the label before the at sign, but emails are still sent to the email address you have specified. For more information, see RFC 1035.

For example, if you enter **test.hostmaster@example.com** when you create the zone, the email address displayed in the SOA record set is **test \.hostmaster.example.com**.

11.1.13 What Is CAA?

Certification Authority Authorization (CAA) is to ensure that HTTPS certificates are issued by authorized certificate authorities (CAs). CAA complies with all IETF RFC 6844 requirements. As of September 8, 2017, all CAs are required to check CAA record sets before they can issue certificates.

CAA Specifications

Domain name owners can create CAA record sets to specify authorized CAs that can issue SSL certificates.

Only authorized CAs can issue SSL certificates for the domain names used by your website. Setting CAA record sets enhances security for your website.

CAs will perform a DNS lookup for CAA record sets when they issue certificates.

- If a CA does not find a CAA record set, the CA can issue a certificate for the domain name.

  Other CAs can also issue certificates for this domain name, but these certificates may be insecure, and there will be messages indicating that your website is insecure when end users access your website.

- If a CA finds a CAA record set that authorizes it to issue certificates, the CA will issue a certificate for the domain name.

- If a CA finds a CAA record set that does not authorize it to issue certificates, the CA will not be able to issue SSL certificates for the domain name.

CAA Record Set

A CAA record set consists of a flag byte **[flag]**, a property tag, and a property value **[tag]-[value]**. You can create multiple CAA record sets for a domain name.

Table 11-2 Configuration of CAA record sets

Function	Example CAA Record Set	Description
Configure a CAA record set for one domain name.	0 issue "ca.example.com"	Only the specified CA (**ca.example.com**) can issue certificates for a particular domain name (**domain.com**). Requests to issue certificates for the domain name by other CAs will be rejected.
	0 issue ";"	No CA is allowed to issue certificates for the domain name (**domain.com**).
Enable a CA to report violations to the domain name holder.	0 iodef "mailto:admin@domain.com"	If a certificate request violates the CAA record set, the CA will notify the domain name holder of the violation.
	0 iodef "http://domain.com/log/" 0 iodef "https://domain.com/log/"	Requests to issue certificates by unauthorized CAs will be recorded.
Authorize a CA to issue wildcard certificates.	0 issuewild "ca.example.com"	The authorized CA (**ca.example.com**) can issue wildcard certificates for the domain name.
Configuration example	0 issue "ca.abc.com" 0 issuewild "ca.def.com" 0 iodef "mailto:admin@domain.com"	A CAA record set is configured for **domain.com**. ● Only CA **ca.abc.com** can issue certificates of all types. ● Only CA **ca.def.com** can issue wildcard certificates. ● Any other CAs are not allowed to issue certificates. ● If a violation occurs, the CA sends a notification to **admin@domain.com**.

Checking Whether a CAA Record Set Has Taken Effect

Use Domain Information Groper (dig) to check whether the CAA record set has taken effect. dig is a network administration command-line tool for querying the Domain Name System. If your OS does not support dig commands, install the dig tool.

Command format: **dig** [*Record set type*] [*Domain name*] **+trace**.

Example command:

dig caa www.example.com +trace

11.1.14 Why Should I Set Priority For an MX Record Set?

The priority you set when you add an MX record set specifies the sequence that an email server receives emails. A smaller value indicates a higher priority.

- If there is only one MX record set, the priority is not applied.
- If there are multiple MX record sets, the DNS server of the email sender preferentially sends emails to the email server with the highest priority.

  If the email server becomes faulty, the DNS server automatically sends emails to the email server with the second highest priority.

For details about how to add MX record sets, see **Managing Record Sets**.

11.1.15 Can DNS Point a Domain Name to a Specific Port?

No. DNS cannot point a domain name to an IP address with a specific port (*Server IP address*:*Port number*).

11.2 Public Zones

11.2.1 How Do I Add Record Sets to Subdomains?

To resolve a subdomain, you need to enter a prefix for the second-level domain name when you configure a record set for it.

The following uses example.com to describe how to add an A record set to its subdomain 123.example.com to map it to an IPv4 address 192.168.1.2.

📖 NOTE

To translate 123.example.com to 192.168.1.2, you need to set the **Name** field to **123** when you add the A record set to example.com. The number of subdomains under a second-level domain name depends on the number of record sets that can be configured for the second-level domain name.

By default, each account can add a maximum of 500 record sets. You can view the number of record sets that can be added above the record set list.

If the quota fails to meet your requirements, contact customer service to request a higher quota.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.
3. In the navigation pane on the left, choose **Public Zones**.

   The **Public Zones** page is displayed.
4. Click the domain name example.com.
5. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
6. Configure the parameters based on **Table 11-3**.

Table 11-3 Parameters for adding an A record set

Parameter	Description	Example Value
Name	Prefix of the second-level domain name. (You do not need to enter the second-level domain name.)	123
Type	Type of the record set.	A – Map domains to IPv4 addresses
TTL (s)	Cache duration of the record set, in seconds.	300
Value	IPv4 addresses mapped to the domain name. Enter each IPv4 address on a separate line.	10.18x.xxx.xxx
Tag	(Optional) Identifier of the record set. Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. For details about tag key and value requirements, see **Table 11-4**.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set.	N/A

Table 11-4 Tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 characters. ● Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Cannot start or end with a space nor contain special characters =*<>\,|/	example_value1

7. Click **OK**.

   You can view the record set you added in the **Normal** state.

11.2.2 Which IP Address Is Returned for the Domain Name If There Are Multiple IP Addresses in a Record Set?

You can configure multiple IP addresses in A and AAAA record sets.

If you have configured multiple IP addresses for an A or AAAA record set, all configured IP addresses will be returned for each query in a random sequence, and the first IP address will be used.

The following describes how a domain name is resolved:

1. An end user enters a domain name in a browser, and the request for the domain name is sent to the local DNS server.
2. The local DNS server forwards the request to the authoritative DNS server.
3. The authoritative DNS server returns all IP addresses to the local DNS server in a random sequence.
4. The local DNS server returns all IP addresses to the browser.
5. The browser uses the first IP address for connection.

Statistically, the probability of returning each IP address is approximately the same.

The following is an example how IP addresses are returned for a domain name. You have a website with a domain name of example.com and deployed on three servers. The IP addresses of the three servers are 192.168.1.1, 192.168.1.2, and 192.168.1.3.

An A record set is configured for example.com, with the **Value** field set to the three IP addresses.

Table 11-5 describes the IP addresses returned when different end users access the website.

Table 11-5 IP addresses returned for the domain name

End User	IP Addresses Returned by the Local DNS Server	IP Address Accessed by the Browser
User A	192.168.1.1 192.168.1.2 192.168.1.3	192.168.1.1
User B	192.168.1.2 192.168.1.1 192.168.1.3	192.168.1.2
User C	192.168.1.3 192.168.1.1 192.168.1.2	192.168.1.3

11.2.3 What Can I Do If There Is Message Indicating that the Public Zone Already Exists?

When you are creating a public zone, there is a message indicating that the public zone has been created by another user.

If you are the holder of the domain name, contact customer service to retrieve you domain name.

11.2.4 Can I Modify a Zone?

Yes. You can modify only the email address and its description of a created zone.

11.2.5 How Can Multiple Domain Names Be Linked to the Same Website?

To access a website using a domain name, host the domain name in the DNS service and configure an A record set to map the domain name to the IP address of the web server where the website is deployed.

To access the same website using other domain names, you need to configure an A record set with the same value for each domain name. **Table 11-6** provides an example.

For details about how to add an A record set, see **Routing Internet Traffic to a Website**.

Table 11-6 Example record sets

Domain Name	Record Set Type	Value
example1.com	A	192.168.1.1
example2.com		

11.2.6 Configuring Weighted Routing

Scenarios

A large website is generally deployed on multiple servers. To balance the load of each server, you can use weights to control the proportion of requests to each server.

The DNS service allows you to set weights to record sets to route the requests to different servers based on the specified weights.

When your website has multiple servers and each server has an independent IP address, consider weighted routing to distribute requests to different servers proportionally.

For example, you have a website deployed on three servers. The domain name of your website is example.com, and the IP addresses of the three servers are 192.168.1.1, 192.168.1.2, and 192.168.1.3.

● If you add an A record set and set its value to the three IP addresses, with no weights set to the IP addresses, requests are randomly routed to an IP address.

For details, see

- You add three A record sets, with each having an IP address as its value.

  In this case, you can set different weights for the three record sets. In this way, requests are routed to each server based on the specified weight.

  Weighted routing can better distribute requests and balance server load. You can perform the operations provided in this section to set the weights.

Constraints

You can configure weights for up to 20 record sets of the same domain name and line.

Preparations

There are three web servers. Three A record sets are required, with the value of each set to the IP address of a web server. You can set different weights to control the proportion of requests to each server.

Table 11-7 Weight setting plans

Plan	Domain Name	Record Set Type	Line Type	Value	Weight	Description
1	example.com	A	Default	192.168.1.1	1	Requests are evenly distributed to three servers (the proportion of requests is 1:1:1).
				192.168.1.2	1	
				192.168.1.3	1	
2	example.com	A	Default	192.168.1.1	2	Requests are distributed to three servers in a proportion of 2:3:1. For example, if there are six requests, two are routed to the server whose IP address is 192.168.1.1, three are routed to the server whose IP address is 192.168.1.2, and one is routed to the server whose IP address is 192.168.1.3.
				192.168.1.2	3	
				192.168.1.3	1	

Prerequisites

The domain name of the website has been hosted on the DNS service.

Procedure

The following describes how to add three A record sets to domain name example.com, and the weight ratio of the three record sets is 1:1:1.

1. Log in to the management console.

2. In the service list, choose **Network** > **Domain Name Service**.

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Public Zones**.

   The **Public Zones** page is displayed.

4. On the **Public Zones** page, click the domain name (**example.com**) of the public zone.

   The **Record Sets** page is displayed.

5. Click **Add Record Set**.

Figure 11-1 Setting weights

6. Configure the parameters as follows:

   – **Name**: Leave this parameter blank. The DNS service automatically considers example.com as the name, and requests are routed to example.com.

   – **Type**: Set it to **A – Map domains to IPv4 addresses**.

   – **Line Type**: Select **Default**.

- **Value**: Set it to **192.168.1.1**, the IP address of a web server.
        - **Weight**: Set it to **1**.
    7. Click **OK**.
    8. Repeat **5** to **7** to add the second and third record sets.

        Set the record set value to 192.168.1.2 and 192.168.1.3, respectively.

        Requests will be evenly distributed to the three servers.

11.3 Private Zones

11.3.1 How Can I Map the Private IP Address of an ECS to a Domain Name?

You can configure PTR records to allow end users to query domain names based on IP addresses.

To map the private IP address of an ECS to a domain name, you must create a private zone and add a PTR record to the zone.

To add a PTR record, you may refer to **Creating a PTR Record**.

📖 **NOTE**

The domain name for the PTR record must be in the *x.x.x.x*.**in-addr.arpa** format. **in-addr.arpa** is the domain name suffix used for reverse resolution.

For example, if the private IP address is 192.168.1.10, the domain name is 10.1.168.192.in-addr.arpa.

You need to create a private zone with the domain name set to 192.in-addr.arpa and add a PTR record with the **Name** field set to **10.1.168**.

Creating a Private Zone

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.

    The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.

    The **Private Zones** page is displayed.
4. Click 📍 in the upper left corner and select the desired region and project.
5. Click **Create Private Zone**.
6. Configure the parameters based on **Table 11-8**.

Table 11-8 Parameters for creating a private zone

Parameter	Description	Example Value
Domain Name	Domain name you use to access the cloud servers or cloud services. Ensure that the domain name suffix is **in-addr.arpa**.	192.in-addr.arpa
VPC	VPC to be associated with the private zone Select the VPC you want to associate with the private zone.	N/A
Email	(Optional) Email address of the administrator managing the private zone. Recommended email address: **HOSTMASTER@***Domain name* For more information about the email address, see **Why Was the Email Address Format Changed in the SOA Record?**	HOSTMASTER@example.com

Parameter	Description	Example Value
Enterprise Project	Enterprise project associated with the private zone. You can manage private zones by enterprise project. **NOTE** This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**. When setting this parameter, note the following: ● If you do not manage zones by enterprise project, select the **default** enterprise project. ● If you manage zones by enterprise project, select an existing enterprise project.	default
Description	(Optional) Supplementary information about the zone You can enter a maximum of 255 characters.	This is a private zone.

7. Click **OK**.
8. Switch back to the **Private Zones** page.

   You can view the created private zone in the list.

   NOTE

   Click the domain name to view SOA and NS record sets automatically generated for the zone.
   ● The SOA record set identifies the primary authoritative server for the domain name.
   ● The NS record set defines the authoritative DNS servers for the domain name.

Adding a PTR Record

1. On the **Private Zones** page, click the domain name of the private zone you created.

The **Record Sets** page is displayed.

2. Click **Add Record Set**.

The **Add Record Set** dialog box is displayed.

3. Configure the parameters based on **Table 11-9**.

Table 11-9 Parameters for adding a PTR record

Parameter	Description	Example Value
Name	Part of the private IP address in reverse order.	10.1.168 For example, if the IP address is 192.168.1.10, the domain name in the PTR record must be 10.1.168.192.in-addr.arpa. ● If the domain name is 192.in-addr.arpa, enter **10.1.168**. ● If the domain name is 1.168.192.in-addr.arpa, enter **10**.
Type	Type of the record set.	PTR – Map IP addresses to domains
TTL (s)	Cache duration of the record set, in seconds.	Default value: 300
Value	Domain name mapped to the IP address. You can enter only one name.	mail.example.com
Description	(Optional) Supplementary information about the PTR record.	The PTR record is for reverse resolution.

4. Click **OK**.

5. Switch back to the **Record Sets** tab.

You can view the added record set in the **Normal** state.

11.3.2 Can I Use Private Domain Names Across Regions?

Private zones are region-level resources. They are created in specified regions and projects.

A private zone can be associated with more than one VPC and takes effect only in its associated VPCs. However, a private zone cannot be used across VPCs. If these VPCs are in the same region and connected over a VPC peering connection, the private zone can be accessed across VPCs.

In the following example, a private zone is created for domain name **example.com**, and it has two VPCs associated and two record sets.

Table 11-10 Record sets added to private zone example.com

Domain Name	Type	Value
ecs1.example.com	A	192.168.1.3
ecs3.example.com	A	192.168.2.3

Figure 11-2 shows how the private domain name is resolved.

Figure 11-2 Process for resolving a private domain name
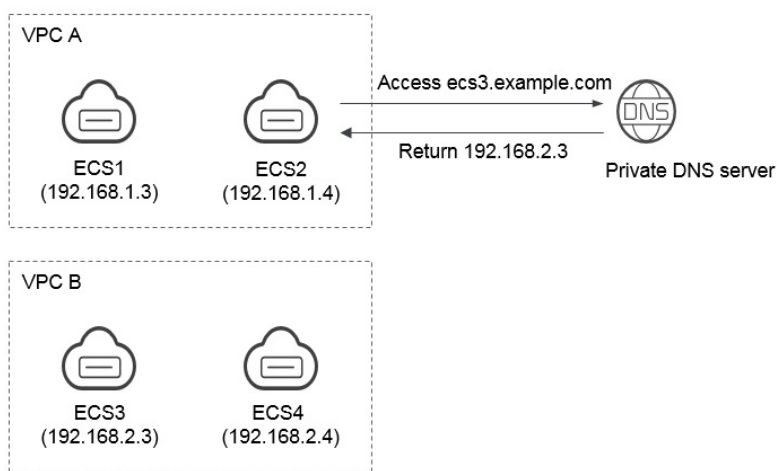
All ECSs in VPC A and VPC B can access example.com.

If ECS 2 in VPC A accesses ecs3.example.com, the private DNS server returns 192.168.2.3, the IP address of ECS 3 in VPC B. There is no VPC peering connection between VPC A and VPC B. ECS 2 cannot access ECS 3 in VPC B using this IP address.

11.3.3 Do I Need to Register Private Domain Names?

Private domain names only take effect in associated VPCs. You do not need to register them.

You can customize any private domain name, other than .com, as long as it complies with domain name specifications. All private domain names are free.

11.3.4 Will a Deleted VPC Be Automatically Disassociated from the Private Zone?

No. Deleted VPCs will not be automatically disassociated from the private zones. If you delete a VPC that has been associated with a private zone, you need to manually disassociate it from the private zone.

11.3.5 Are Private DNS Server Addresses the Same for All Users?

Private DNS server addresses are the same in the same AZ, and private domain names of each user are logically isolated.

11.3.6 What Are the Restrictions on Concurrent Private DNS Requests?

To ensure the lookup efficiency of private domain names, only 2,000 queries are allowed on a single source IP address per second. If a server initiates DNS queries with an overwhelmingly high frequency, significantly in excess of normal service demands, and there are more than 2,000 queries per second, additional queries will not be processed.

If your services initiate an enormous volume of concurrent requests, enable DNS caching to improve lookup efficiency.

11.4 Reverse Resolution

11.4.1 What Is Reverse Resolution?

Generally, DNS resolves a domain name to an IP address. When you access a website using a domain name, DNS maps the domain name to the IP address of the web server where the website is deployed.

Reverse resolution, on the opposite, is a query in which a domain name connected with an IP address is returned. It is usually used in scenarios such as anti-spam and logging.

- Anti-spam: queries the domain name based on the IP address of the sender's mail server to obtain the reputation of the domain name.
- Logging: queries the domain name or host name based on the IP address to distinguish service data.

To obtain a domain name from a private IP address, you need to create a private zone for top-level domain in-addr.arpa. For example, if the IP address 192.0.2.255, the domain name for the PTR record can be 255.2.0.192.in-addr.arpa.

A Change History

Released On	Description
2023-11-30	This issue is the sixth official release, which incorporates the following changes: ● Added system-defined policy DNS ReadOnlyAccess in **Table 1-1** and **Table 1-2** of **Permissions**. ● Updated screenshots in **Procedure**, **Creating a Private Zone**, and **Procedure**. ● Updated screenshots for **Procedure** and added **Enterprise Project** in **Table 3-2**. ● Updated screenshots for **Procedure** and added **Enterprise Project** in **Table 4-2**. ● Added **Weight** in **Table 5-3**, **Table 5-5**, **Table 5-6**, **Table 5-7**, **Table 5-8**, **Table 5-9**, **Table 5-10**, and **Table 5-11**. ● Added **Intelligent Resolution**. ● Added **Configuring Weighted Routing**.
2023-06-15	This issue is the fifth official release, which incorporates the following changes: ● Added **Figure 1-7**. ● Updated **Table 1-3**. ● Updated **Project**.

Released On	Description
2023-04-30	This issue is the fourth official release, which incorporates the following changes: ● **Permissions** ● **Project** ● **Permissions Management** ● **What Are DNS Servers?** ● **What Are the Differences Between Public and Private Domain Names?** ● **Does DNS Support IPv6?** ● **Does DNS Support Explicit and Implicit URLs?** ● **Does DNS Support Dynamic Domain Name Resolution?** ● **What Is TTL?** ● **How Many Domain Name Levels Does DNS Support?** ● **Why Should I Set Priority For an MX Record Set?** ● **How Do I Add Record Sets to Subdomains?** ● **Which IP Address Is Returned for the Domain Name If There Are Multiple IP Addresses in a Record Set?** ● **Can I Modify a Zone?** ● **How Can Multiple Domain Names Be Linked to the Same Website?** ● **Can I Use Private Domain Names Across Regions?** ● **Do I Need to Register Private Domain Names?** ● **Will a Deleted VPC Be Automatically Disassociated from the Private Zone?** ● **Are Private DNS Server Addresses the Same for All Users?** ● **What Are the Restrictions on Concurrent Private DNS Requests?** ● **Reverse Resolution**
2021-03-24	This issue is the third official release, which incorporates the following changes: Added record sets of the CAA type in the following topics: ● **Record Set** ● **Record Set Types and Configuration Rules** ● **Adding a CAA Record Set** ● **What Is CAA?**
2020-12-11	This issue is the second official release, which incorporates the following changes: Optimized the operation scenarios in this document.
2018-08-15	This issue is the first official release.