Domain Name Service

User Guide

Date   2020-02-26

Contents

1 Overview

1.1 What Is DNS?

Domain Name Service (DNS) route queries for private domain names to facilitate access to cloud resources within the VPCs.

With DNS, you can

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

Product Advantages

The DNS service has the following advantages:

- High performance

  DNS can handle millions of concurrent queries on a single node, allowing your end users to quickly access the closest application endpoints that are healthy.

- Easy access to cloud resources

  You can host private domain names so that your ECSs can communicate with each other or with resources within VPCs using private domain names. Traffic is not directed to the Internet, and this reduces network latency and improves security.

- Isolation of core data

  A private DNS server provides domain name resolution for ECSs carrying core data, enabling communications while safeguarding the core data. You do not need to bind EIPs to these ECSs.

How to Access

The cloud platform provides a web-based management console and 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 Private Zone

What Is a Private Zone?

A private zone contains information about how to map domain names used within VPCs such as ecs.com to private IP addresses such as 192.168.1.1. With private domain names, your ECSs can communicate with each other within the VPCs without having to connect to the Internet. You can also access cloud services, such as OBS and SMN, via the private DNS server.

Figure 1-1 shows the process how a private domain name is resolved.

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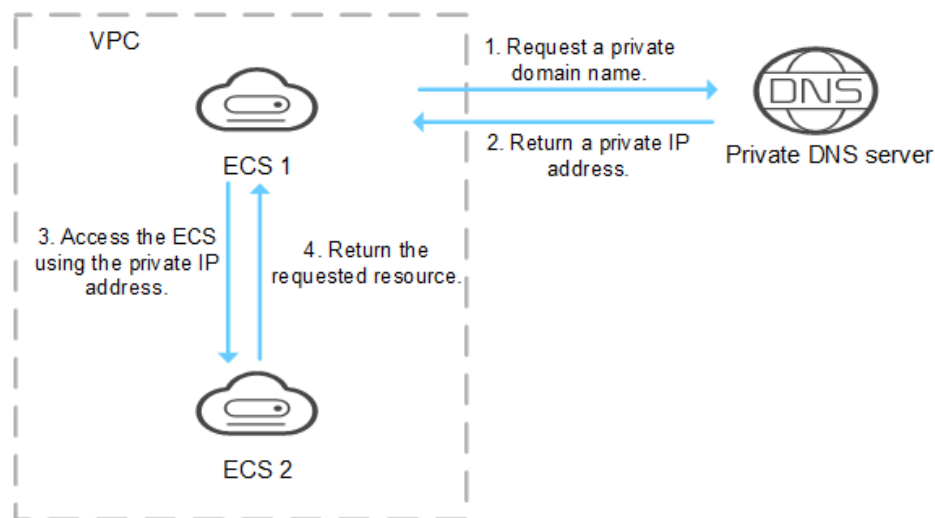
When an ECS in the VPC requests a private domain name, the private DNS server directly returns a private IP address mapped to the domain name.

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 RDS resources.

You can use private domain names in the following scenarios:

- **Managing ECS Host Names**
- **Replacing an ECS Without Service Interruption**
- **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 **Configuring a Private Zone** for detailed operations.

Replacing an ECS Without Service Interruption

As the number of Internet users is continuously increasing, a website application deployed only on one server can hardly handle concurrent requests during business spikes. A common practice is to deploy the application on multiple servers and distribute the load across 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 ECSs. If one server is replaced in the system, its private IP address changes accordingly. 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 in the VPCs and map their host names to private IP addresses, they will be able to communicate using private domain names. When you replace any of the ECSs, you only need to change the IP address in record sets, instead of modifying the code.

Figure 1-2 shows a typical scenario of private zones.

Figure 1-2 Configuring private DNS for cloud servers
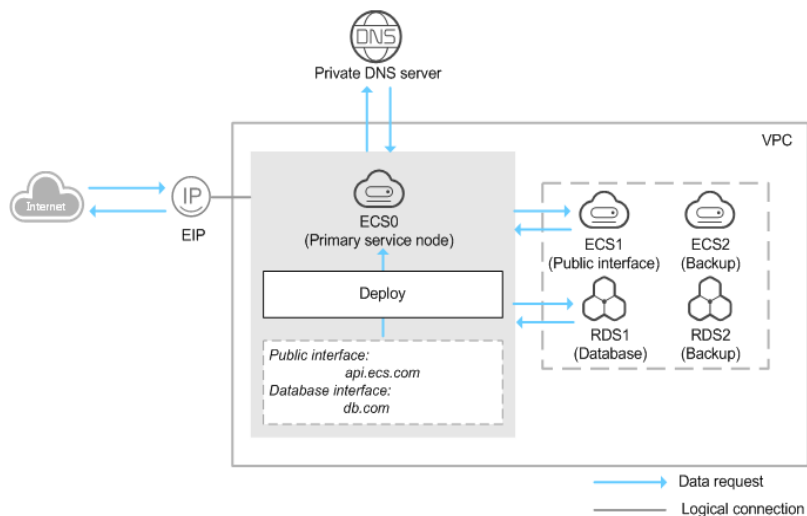
ECSs and RDS instances are in the same VPC.

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

When ECS1 becomes faulty, the backup server ECS2 must work instead. However, if no private domain names 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 domain names for the ECSs and have included these domain 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 subnet where the ECS resides and the VPC of this subnet has been associated with a private zone, requests to access cloud services will be routed over the Internet.

  Figure 1-3 shows the process for resolving a domain name when an ECS accesses cloud services.

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

- If a private DNS server is configured for the subnet, it directly processes the requests to access cloud resources.

  When the ECS accesses these 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 1-3** shows the process.

Figure 1-3 Accessing cloud services
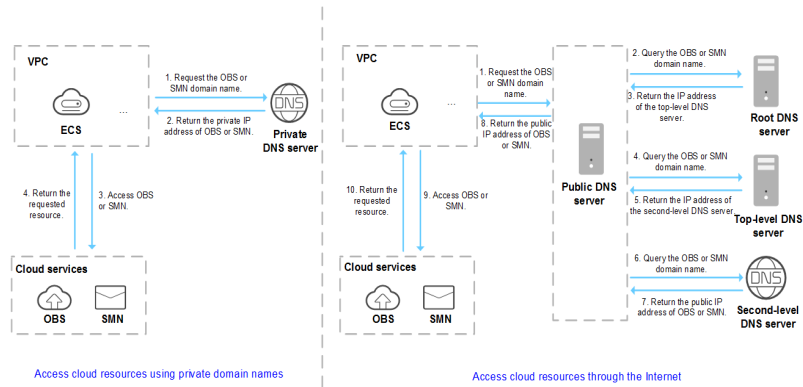
1.3 Functions

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

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

Table 1-1 Common DNS functions

Category	Function	Description
Private domain resolution	Private zone	You can create private domain names that take effect in associated VPCs. DNS allows you to create, modify, delete, and view private zones, associate private zones with VPCs, and disassociate private zones from VPCs. ● Private zones can be created without registering domain names. ● The private zone must be unique in the associated VPC. For details, see **Overview**.
	Associating a private zone with or disassociating a private zone from a VPC	You can associate a private zone with or disassociate a private zone from a VPC. For details, see **Associating a VPC with a Private Zone** and **Disassociating a VPC from a Private Zone**.

Category	Function	Description
	Record set	A record set is a group of resource records that define the resolution type and value of a domain name. You can add, modify, delete, or view A, CNAME, MX, AAAA, TXT, PTR, and SRV record sets for private zones. For details, see **Overview**.
	Wildcard resolution	You can add record sets for all subdomains of a private zone. DNS provides resolution services for all subdomains. For details, see **Creating a Wildcard DNS Record Set**.
	TTL	TTL is short for time-to-live, which specifies the cache period of resource records on a local DNS server. The TTL value ranges from 1 to 2147483647.
	Batch deleting private zones	You can delete multiple private zones at a time.
Record sets	Searching for record sets globally	DNS allows you to centrally manage record sets, including the following: ● Searching for record sets by status, type, name, value, ID, or tag ● Modifying or deleting record sets of private zones For details, see **Searching for Record Sets Globally**.
Tag	Resource tag	You can configure tags for private zones and record sets. You can also use predefined tags provided by Tag Management Service (TMS) to quickly associate tags with resources.
Quota	Quota adjustment	Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number of resources available to users, for example, the maximum number of zones or record sets that you can create. If the existing resource quota cannot meet your service requirements, you can apply for a higher quota. For details, see **Quota Adjustment**.

1.4 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your DNS resources, IAM is an ideal choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your cloud resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use DNS resources but should not be able delete the resources or perform any other high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using specific resources.

Skip this section if your account does not require individual IAM users for permissions management.

IAM free of charge. You pay only for cloud resources you purchase or use.

DNS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services.

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.

To assign permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing the DNS service, users need to switch to a region where they have been authorized to use DNS resources.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you need to also assign other roles on which the permissions depend, for the permissions to take effect. However, roles are not ideal for fine-grained authorization and secure access control.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, and meets the requirements for secure access control. For example, you can grant DNS users only the permissions for managing a

certain type of DNS resources. Most policies define permissions based on APIs. For the API actions supported by the DNS service, see Permissions Policies and Supported Actions in the *Domain Name Service API Reference*.

Table 1-2 lists all system-defined roles or policies supported by DNS.

Table 1-2 DNS roles or policies

Role/Policy Name	Description	Type	Dependency
DNS FullAccess	All permissions on DNS.	System-defined policy	None
DNS ReadOnlyAccess	Read-only permissions for DNS. Users granted with these permissions can only view DNS resources.	System-defined policy	None
DNS Administrator	All permissions on DNS.	System-defined role	This role depends on the **Tenant Guest** and **VPC Administrator** roles in the same project.

Table 1-3 lists the common operations supported by each DNS system policy or role. Choose proper system policies according to this table.

Table 1-3 Common operations supported by each system-defined DNS policy or role

Operation	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
Creating a private zone	√	x	√
Viewing a private zone	√	√	√
Modifying a private zone	√	x	√
Deleting a private zone	√	x	√
Deleting private zones in batches	√	x	√
Associating a VPC with a private zone	√	x	√
Disassociating a VPC from a private zone	√	x	√

Operation	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
Adding a record set	√	x	√
Viewing a record set	√	√	√
Modify a record set	√	x	√
Deleting a record set	√	x	√
Delete record sets in batches	√	x	√
Exporting record sets in batches	√	x	√
Importing record sets in batches	√	x	√

Related References

- *Identity and Access Management User Guide*
- **Creating a User and Granting DNS Permissions**
- Section "Permissions Policies and Supported Actions" in the *Domain Name Service API Reference*

1.5 Related Services

Table 1-4 shows the relationships between DNS and other services.

Table 1-4 Related services

Description	Related Service	Reference
Create VPCs for the DNS service.	Virtual Private Cloud (VPC)	**Configuring a Private Zone**
Record operations performed on the DNS service	Cloud Trace Service (CTS)	**DNS Operations Recorded by CTS**

1.6 Product Concepts

1.6.1 Domain Name Format and Structure

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.

Domain names are classified into the following levels based on their 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.

1.6.2 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 1-5 describes the record set types and their application scenarios.

Table 1-5 Record set usages

Type	Usage
A	Maps domains to IPv4 addresses.
CNAME	Maps one domain name to another or multiple domain names to one domain name.
MX	Maps domain names to email servers.
AAAA	Maps domain names to IPv6 addresses.
TXT	Specifies text records. TXT record sets are 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.
SRV	Records servers providing specific services.

Type	Usage
NS	Delegates subdomains to other name servers. This type of record sets is created by default and cannot be manually added.
SOA	Specifies the master authoritative DNS server for a domain name. The SOA record set is created by the system and cannot be added manually.
PTR	Maps IP addresses to domain names.

### Usage

Record sets are used in following scenarios:

- Private domain name resolution

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

  Figure 1-4 Private domain name resolution

- Reverse resolution on a private network

  You can use PTR records to translate private IP addresses into private domain names.

  Figure 1-5 Reverse resolution on a private network
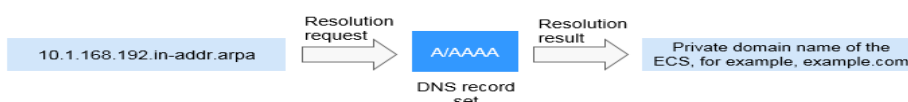
Helpful Links

For details, see **Overview**.

1.6.3 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 1-6 shows the relationship between regions and AZs.

Figure 1-6 Regions and AZs
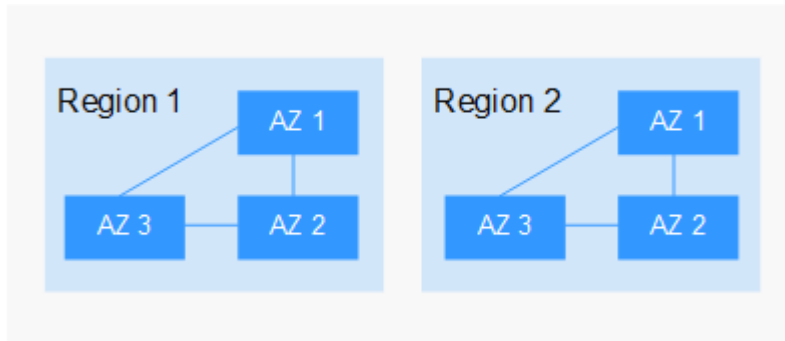
Selecting a Region

Select a region closest to your target users for low 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 low 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**.

1.6.4 Project

Projects are used to group and isolate OpenStack 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.

Private zones are region-level resources. Therefore, private zones are isolated and managed based on projects. You need to create, query, and configure private zones in specific regions and projects.

2 Getting Started

2.1 Configuring a Private Zone

Scenarios

If you have deployed ECSs and other cloud services on the cloud, you can configure private domain names for the ECSs so that they can communicate using domain names within VPCs.

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

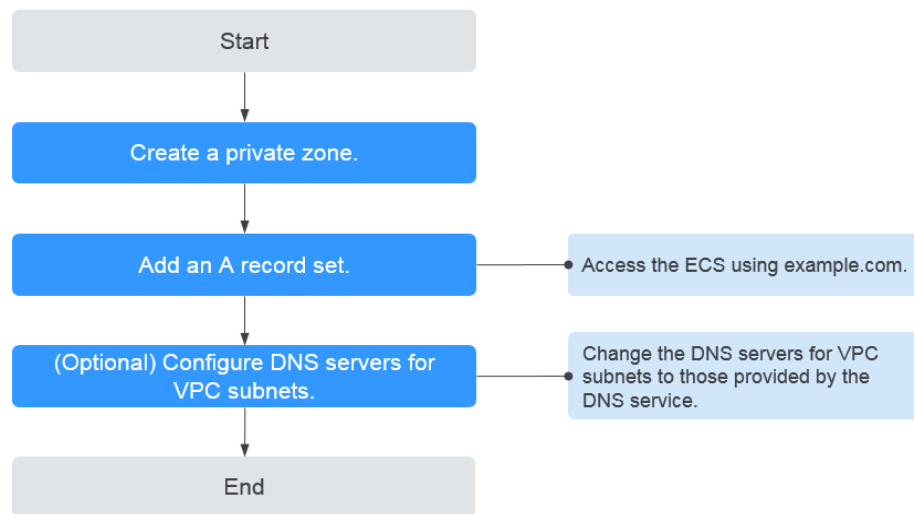This section describes how to configure a private zone for a private domain name and add an A record set.

Prerequisites

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

Process

Figure 2-1 shows the process for configuring a private zone for a domain name.

Figure 2-1 Process for configuring a private zone

Create a Private Zone

Create a private zone to allow access to your ECS using a private 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, 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 **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.

    View the created private zone.

    📖 NOTE

    Click the zone name to view detailed zone information. You can view SOA and NS record sets created by the system.
    - The SOA record set defines the DNS server that is the authoritative information source for a particular domain name.
    - The NS record set defines authoritative DNS servers for a zone.

Add an A Record Set

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

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

    The **Record Sets** page is displayed.

2. Click **Add Record Set**.
3. Set the parameters as follows:
   – **Name**: Leave this parameter blank. The system automatically considers example.com as the name, and requests are routed to example.com.
   – **Type**: Set it to **A – Map domains to IPv4 addresses**.
   – **Value**: Enter the private IP address of the ECS.

   Retain the default values for other parameters. For details, see **Adding an A Record Set**.
4. Click **OK**.
5. Switch back to the **Record Sets** page.

   View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

(Optional) Configure DNS Servers for the VPC Subnet

To ensure that private domain names can be resolved in a VPC, change the DNS servers for the VPC subnet to those provided by the DNS service.

Query the private DNS servers 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, 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 name of the zone and view the DNS servers.

Change the DNS servers

1. Go to the private zone list.
2. Click the VPC name under **Associated VPC**.

   On the VPC console, change the DNS servers of the VPC subnet.

   For details, see "Modifying a Subnet" in the *Virtual Private Cloud User Guide*.

3 Private Zone

3.1 Overview

Private zones provide configurations for private domain names that are only applicable within VPCs, and they map private domain names to private IP addresses and resolve domain names within VPCs.

- 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.

This chapter describes how to create and manage private zones.

Table 3-1 Private zone operations

Operation	Description	Constraint
Creating a Private Zone	Create a 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 a maximum of 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.

Operation	Description	Constraint
Managing Private Zones	Modify, delete, and query private zones.	• The name of a private zone cannot be modified after the zone is created. • After a private zone is deleted, all its record sets will also be deleted.
Associating a VPC with a Private Zone	Configure private domain names for VPCs.	• 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.

3.2 Creating a Private Zone

Scenarios

Create a private zone to resolve a private domain name within VPCs.

Prerequisites

- You have created a VPC.
- You have created an ECS in the VPC and planned a domain name (example.com) planned 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, 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 the required parameters.
   Table 3-2 describes the parameters.

Table 3-2 Parameters for creating a private zone

Parameter	Description	Example Value
Name	Name of the private zone, which is the private 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 the servers are deployed. Otherwise, the domain name cannot be resolved.	-
Email	(Optional) Email address of the administrator managing the private zone It is recommended that you set the email address to **HOSTMASTER@*Domain name***. For more information about the email address, see **Why Is the Email Address Format Changed in the SOA Record?**	HOSTMASTER@example.com
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. Before you set this parameter, create an enterprise project by referring to **Creating an Enterprise Project**.	default

Parameter	Description	Example Value
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a zone. For details about tag key and value requirements, see **Table 3-3**.	example_key1 example_value1
Description	(Optional) Supplementary information about the zone You can enter a maximum of 255 characters.	This is a zone example.

Table 3-3 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.	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters.	example_value1

7. Click **OK**.

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

   View the created private zone in the zone list.

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

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

   📖 NOTE

   Click the zone name to view detailed zone information. You can view SOA and NS record sets created by the system.

   ● The SOA record set defines the DNS server that is the authoritative information source for a particular domain name.

   ● The NS record set defines authoritative DNS servers for a 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 **Overview**.

● Modify or delete it, or view its details. For details, see **Managing Private Zones**.

3.3 Managing Private Zones

Scenarios

You can view details of a private zone, modify a private zone, or delete a private zone.

Modifying a Private Zone

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

📖 **NOTE**

> For more information about the email address, see **Why Is 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, 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 click **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, 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 click **Delete** under **Operation**.

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

6. Click **Yes**.

Batch Deleting Private Zones

Delete multiple private zones at a time. After the private zones are deleted, domain names and their subdomains cannot be resolved by the DNS service.

NOTICE

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

----

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 **Private Zones**.

   The **Private Zones** page is displayed.

4. Click ⦿ in the upper left corner and select the desired region and project.
5. Select the private zones you want to delete and click **Delete**.
6. In the **Delete Private Zone** dialog box, click **Yes**.

Viewing Details About a Private Zone

View details about a private zone, such as zone ID, operation time, tag, 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. Locate the private zone you want to view and click ⌄ before the zone name to view its details.

3.4 Associating a VPC with a Private Zone

Scenarios

Associate a VPC with a private zone so that the private domain name can work in this VPC.

📖 **NOTE**

This VPC must be the same as the VPC where the servers are deployed. Otherwise, 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, 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**.

3.5 Disassociating a VPC from a Private Zone

Scenarios

Disassociate a VPC from a private zone if you do not want to the private domain name to work 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.

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 **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**.

4 Record Set

4.1 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 4-1 Record set management

Operation	Scenario	Constraint
Record Set Types and Configuration Rules	View record set types supported by the DNS service and their configuration rules.	None
Adding Record Sets	Add record sets to a domain name. For details, see **Table 4-2**.	• 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, delete, or disable SOA and NS record sets automatically created by the system.
Creating a Wildcard DNS Record Set	Add a record set that matches all subdomains.	Wildcard DNS resolution does not support NS record sets.

Operation	Scenario	Constraint
Searching for Record Sets	Search for, modify, disable, and delete record sets on the **Dashboard** > **Record Set** page.	None
Importing Record Sets	Batch import record sets.	● Record sets are listed in **.xlsx** files, and each file cannot exceed 2 MB. ● A maximum of 500 record sets can be imported at a time.
Exporting Record Sets	Batch export record sets.	None

Figure 4-1 shows the process for configuring a record set on the DNS console.

Figure 4-1 Process for configuring a record set
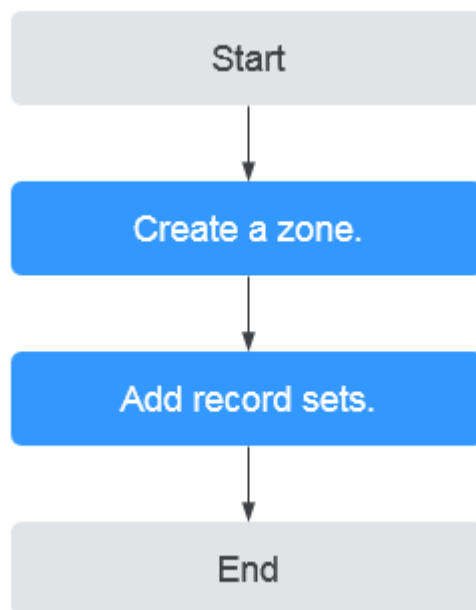
4.2 Record Set Types and Configuration Rules

Type

Table 4-2 describes the record set types.

Table 4-2 Record set types

Type	Description
A	Maps domains to IPv4 addresses.
CNAME	Maps one domain name to another or multiple domain names to one domain name.
MX	Maps domain names to email servers.
AAAA	Maps domain names to IPv6 addresses.
TXT	Specifies text records. 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.
SRV	Records servers providing specific services.
SOA	Specifies the master authoritative DNS server for a domain name. The SOA record set is created by the system and cannot be added manually.
PTR	Maps IP addresses to domain names.

Record Set Configuration

Table 4-3 lists the value requirements for different types of record sets.

Table 4-3 Requirements for record set values

Record Set Type	Value	Example
A	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	Domain name alias. You can enter only one domain name.	www.example.com

Record Set Type	Value	Example
MX	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.
AAAA	IPv6 addresses mapped to the domain name You can enter a maximum of 50 record values, each on a separate line.	ff03:0db8:85a3:0:0:8a2e:0370:7334
TXT	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	Value	Example
SRV	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 priority value indicates a higher priority. ● A larger weight 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** The system checks the priority values first. If the priority values are the same, the system will check the weight values.	2 1 2355 example_server.test.com
PTR	Private domain name mapped to the private IP address. You can enter only one domain name.	www.example.com.

4.3 Adding Record Sets

4.3.1 Adding an A Record Set

Scenarios

If you want to use a private domain name to access ECSs configured with IPv4 addresses, you can add an A record set for the domain name.

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

Prerequisites

You have an ECS 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 **Private Zones**.

 The zone list is displayed.

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

5. Click the zone name.

6. Click **Add Record Set**.

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

7. Set required parameters based on **Table 4-4**.

Table 4-4 Parameters for adding an A record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved For example, if the zone name is **example.com**, the domain name 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. ● **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 an email server. ● *****: 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 If a message is displayed indicating that the record set you are trying to create exists, the record set 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.	The default value is **300**, which is, 5 minutes.

Parameter	Description	Example Value
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
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. This parameter is displayed when you enable **Other Settings**. For details about tag key and value requirements, see **Table 4-5**.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set You can enter a maximum of 255 characters.	N/A

Table 4-5 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.	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters.	example_value1

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

   View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

Related Operations

For more information about how to configure A record sets, see **Configuring a Private Zone**.

4.3.2 Adding an AAAA Record Set

Scenarios

If you want to use a domain name to access websites, web applications, or cloud servers configured with IPv6 addresses, you can add an AAAA record set for the domain name.

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

Prerequisites

You have an ECS 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 **Private Zones**.

   The zone list is displayed.
4. Click in the upper left corner and select the desired region and project.
5. Click the zone name.
6. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
7. Set required parameters based on **Table 4-6**.

Table 4-6 Parameters for adding an AAAA record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved For example, if the zone name is **example.com**, the domain name 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. • **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 an email server. • *****: 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 If a message is displayed indicating that the record set you are trying to create exists, the record set 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.	The default value is **300**, which is, 5 minutes.
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: 0370:7334
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. This parameter is displayed when you enable **Other Settings**. For details about tag key and value requirements, see **Table 4-7**.	example_key1 example_valu e1
Description	(Optional) Supplementary information about the record set You can enter a maximum of 255 characters.	-

Table 4-7 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.	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters.	example_value 1

8. Click **OK**.

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

    View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

4.3.3 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 **Private Zones**.
   The zone list is displayed.
4. Click ⓥ in the upper left corner and select the desired region and project.
5. Click the zone name.
6. Click **Add Record Set**.
   The **Add Record Set** dialog box is displayed.
7. Set required parameters based on **Table 4-8**.

Table 4-8 Parameters for adding a CNAME record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved For example, if the zone name is **example.com**, the domain name 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. ● **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 an email server. ● *****: 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 If a message is displayed indicating that the record set you are trying to create exists, the record set 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.	The default value is **300**, which is, 5 minutes.
Value	Domain name alias. You can enter only one domain name.	webserver01.example.com
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. This parameter is displayed when you enable **Other Settings**. For details about tag key and value requirements, see **Table 4-9**.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set You can enter a maximum of 255 characters.	-

Table 4-9 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.	example_key1
Value	• Cannot be left blank. • Can contain a maximum of 43 characters.	example_value1

8. Click **OK**.

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

   View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

4.3.4 Adding an MX Record Set

Scenarios

If you want to specify email servers mapped 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 **Private Zones**.

   The zone list is displayed.

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

5. Click the zone name.

6. Click **Add Record Set**.

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

7. Set required parameters based on **Table 4-10**.

Table 4-10 Parameters for adding an MX record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved For example, if the zone name is **example.com**, the domain name 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. ● **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 an email server. ● *****: 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 If a message is displayed indicating that the record set you are trying to create exists, the record set 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.	The default value is **300**, which is, 5 minutes.
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

Parameter	Description	Example Value
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. This parameter is displayed when you enable **Other Settings**. For details about tag key and value requirements, see **Table 4-11**.	example_key1 example_value 1
Description	(Optional) Supplementary information about the record set You can enter a maximum of 255 characters.	The description of the hostname.

Table 4-11 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.	example_key1
Value	• Cannot be left blank. • Can contain a maximum of 43 characters.	example_value 1

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

   View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

4.3.5 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 **Private Zones**.

   The zone list is displayed.

4. Click ⊙ in the upper left corner and select the desired region and project.
5. Click the zone name.
6. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
7. Set required parameters based on **Table 4-12**.

Table 4-12 Parameters for adding a TXT record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved For example, if the zone name is **example.com**, the domain name 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. ● **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 an email server. ● *****: 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 If a message is displayed indicating that the record set you are trying to create exists, the record set 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.	The default value is **300**, which is, 5 minutes.

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"
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. This parameter is displayed when you enable **Other Settings**. For details about tag key and value requirements, see **Table 4-13**.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set You can enter a maximum of 255 characters.	-

Table 4-13 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.	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters.	example_value1

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

View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

4.3.6 Adding an SRV Record Set

Scenarios

To record services provided by a server, 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 **Private Zones**.

    The zone list is displayed.
4. Click in the upper left corner and select the desired region and project.
5. Click the zone name.
6. Click **Add Record Set**.

    The **Add Record Set** dialog box is displayed.
7. Set required parameters based on **Table 4-14**.

Table 4-14 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 If a message is displayed indicating that the record set you are trying to create exists, the record set conflicts with an existing record set.	SRV – Record servers providing specific services

Parameter	Description	Example Value
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.	The default value is **300**, which is, 5 minutes.
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 priority value indicates a higher priority. ● A larger weight 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** The system checks the priority values first. If the priority values are the same, the system will check the weight values.	2 1 2355 example_server.test.com
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. This parameter is displayed when you enable **Other Settings**. For details about tag key and value requirements, see **Table 4-15**.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set You can enter a maximum of 255 characters.	-

Table 4-15 Tag key and value requirements

Paramete r	Requirements	Example Value
Key	- Cannot be left blank. - Must be unique for each resource. - Can contain a maximum of 36 characters.	example_key1
Value	- Cannot be left blank. - Can contain a maximum of 43 characters.	example_value 1

8. Click **OK**.

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

   View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

4.3.7 Adding a PTR Record

Scenarios

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

For details about other record set types, see **Overview**.

Constraints

- You can create PTR records only in private zones.
- PTR records take effect only in a private zone whose domain name suffix is in-addr.arpa.

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 **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 zone name.

6. Click **Add Record Set**.

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

7. Set required parameters based on **Table 4-16**.

Table 4-16 Parameters for adding a PTR record

Parameter	Description	Example Value
Name	Name of the PTR record	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 name is 192.in-addr.arpa, enter **10.1.168** in the box. ● If the private zone name is 1.168.192.in-addr.arpa, enter **10** in the box.
Type	Type of the record set If a message is displayed indicating that the record set you are trying to create exists, the record set 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.	The default value is **300**, which is, 5 minutes.
Value	Private domain name mapped to the private IP address. You can enter only one domain name.	host.example.com.

Parameter	Description	Example Value
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. This parameter is displayed when you enable **Other Settings**. For details about tag key and value requirements, see **Table 4-17**.	example_key1 example_value 1
Description	(Optional) Supplementary information about the record set You can enter a maximum of 255 characters.	-

Table 4-17 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.	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters.	example_value 1

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

   View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

Related Operations

For more information, see **How Can I Configure a PTR Record for the Private IP Address of an ECS?**

4.4 Managing Record Sets

Scenarios

You can modify, delete, disable, or enable 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 by the system and cannot be deleted.

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 **Private Zones**.

   The zone list is displayed.

4. Click ◎ in the upper left corner and select the desired region and project.
5. Click the zone 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 by the system 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 **Private Zones**.

   The zone list is displayed.

4. Click ◎ in the upper left corner and select the desired region and project.
5. Click the zone 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**.

Batch Deleting Record Sets

Delete multiple record sets at a time. Deleted record sets cannot be recovered, and domain name queries will fail.

NOTE

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

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 **Private Zones**.
   The zone list is displayed.
4. Click ⦿ in the upper left corner and select the desired region and project.
5. Select the record sets you want to delete and click **Delete**.
6. 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 **Private Zones**.
   The zone list is displayed.
4. Click ⦿ in the upper left corner and select the desired region and project.
5. Click the zone name.
   The **Record Sets** page is displayed.
6. Locate the record set you want to view and click ⌄ before its name.

4.5 Creating a Wildcard DNS Record Set

Scenarios

A wildcard DNS record set is used to match requests for all subdomains in a zone. You can add a record whose name is an asterisk (*) to resolve requests to all subdomains of the domain name to the same value.

This section describes how to create a wildcard DNS record set.

Constraints

Wildcard DNS resolution does not support NS 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 **Private Zones**.

The zone list is displayed.

4. Click ⊙ in the upper left corner and select the desired 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. Set the parameters based on **Table 4-18**.

Table 4-18 Parameters for adding a wildcard DNS record set

Parameter	Description	Example Value
Name	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 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.	The default value is **300**, which is, 5 minutes.
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
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. This parameter is displayed when you enable **Other Settings**. For details about tag key and value requirements, see **Table 4-19**.	example_key1 example_value1

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.

Table 4-19 Tag key and value requirements

Paramete r	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 characters.	example_key1
Value	• Cannot be left blank. • Can contain a maximum of 43 characters.	example_value 1

8. Click **OK**.

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

   View the created wildcard DNS record set in the record set list of the domain name, and ensure that the status of the record set is **Normal**.

4.6 Searching for Record Sets

Scenarios

The DNS service allows you to centrally manage record sets in private zones.

You can quickly search for record sets by its status, type, name, value, tag, or ID.

In the following operations, record sets of a private zone are used as an example.

Procedure

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 **Record Sets**.

   The record set list is displayed.

4. Click **Private Zone Record Sets**.

5. Set search criteria to search for record sets.

   The following search criteria are available:

- – **Status**: Search for record sets in a specified state.
- – **Type**: Search for record sets of a specified type.
- – **Name**: Search for record sets by domain name.
- – **Value**: Search for record sets based on their values.
- – **ID**: Search for record sets based on their IDs.
- – **Search by Tag**: Search for record sets based on preset tags.

6. Click ⌄ before the domain name to view the record set details.

7. Click **Modify** or **Delete** to perform desired record set operations.

4.7 Importing Record Sets

Scenarios

If you want to transfer your domain names from other cloud provider to the DNS service for management, you can import existing record sets in batches.

You can import a maximum of 500 record sets at a time.

☐ **NOTE**

Before importing record sets, you have created private zones on the DNS console. For details, see **Creating a Private Zone**.

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 **Private Zones**.

The zone list is displayed.

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

5. In the zone list, click the zone name **example.com**.

6. Choose **Export and Import**.

   a. Click **Download template**.

   b. List your record sets as required in the template.

   ☐ **NOTE**

   Ensure that the content is imported based on the format of the template. Otherwise, the import will fail.

7. Click **Import Record Set** and select the record set file to import.

   After the import is complete, you can check whether record sets are successfully imported or not.

   - – **Succeeded Import**: The number of successfully imported record sets are displayed.

   - – **Failed Import**: All failed record sets are listed. You can resolve the problems based on the failure causes.

4.8 Exporting Record Sets

Scenarios

If you want to transfer your domain name from the DNS service to other cloud provider, you can export your record sets.

This section uses the domain name example.com as an example.

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 **Private Zones**.
   The zone list is displayed.

4. Click in the upper left corner and select the desired region and project.
5. In the zone list, click the zone name **example.com**.
6. Choose **Export and Import**.
7. Click **Export Record Set**.
   An **example.com.xlsx** file is exported, which lists all record sets in the zone, including the record set name, type, TTL, and value.

5 Permissions Management

5.1 Creating a User and Granting DNS Permissions

This chapter describes how to use IAM to implement fine-grained permissions control for your DNS resources. 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.

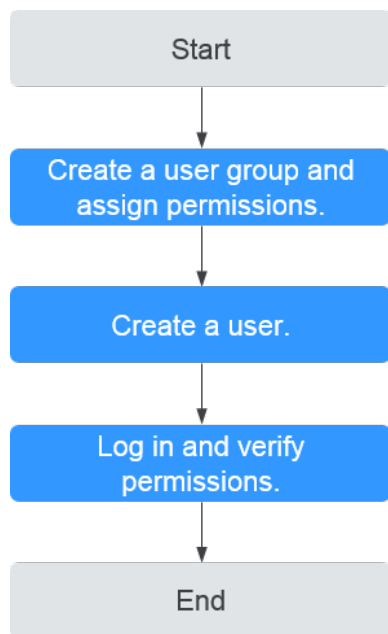If your account does not need individual IAM users, skip this section.

This section describes the procedure for granting permissions (see **Figure 5-1**).

Prerequisites

Learn about the permissions.

Process Flow

Figure 5-1 Process for granting permissions

1. Create a user group and grant permissions.

   Create a user group on the IAM console and attach the **DNS ReadOnlyAccess** policy to the group, which grants users read-only permissions to DNS resources.

2. Create an IAM user.

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

3. Log inand verify permissions.

   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 DNS console, choose **Dashboard** > **Private Zones**. On the displayed page, click **Create Private Zone**. If the private zone cannot be created, the **DNS ReadOnlyAccess** policy has already taken effect.

   – Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **DNS ReadOnlyAccess** policy has already taken effect.

5.2 Creating Custom Policies

You can create custom policies to supplement system-defined policies and implement more refined access control.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.

● JSON: Edit JSON policies from scratch or based on an existing policy.

The following describes how to create a custom policy that allows users to modify DNS zones in the visual editor and JSON view.

For details, see . The following section contains examples of common DNS custom policies.

Creating a Custom Policy in the Visual Editor

1. Log in to the management console.

2. On the management console, hover over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.

3. In the left navigation pane, choose Permissions.

4. Click **Create Custom Policy**.

   The **Create Custom Policy** page is displayed.

5. Enter a policy name.

6. Select a scope in which the policy will take effect based on the type of services to be set in this policy.

   – **Global services**: Select this option if the services to which the policy is related are available for all regions once deployed. When creating custom policies for globally deployed services, specify the scope as **Global services**. Custom policies of this scope must be attached to user groups in the Global service region.

   – **Project-level services**: Select this option if the services to which the policy is related are deployed in specific regions. When creating custom policies for regionally deployed services, specify the scope as **Project-level services**. Custom policies of this scope must be attached to user groups in specific regions except the Global service region.

   Select **Project-level services** here.

   📖 NOTE

   A custom policy can contain actions of multiple services that are all globally available or all deployed only in specific projects. To define permissions required for accessing both globally available and project-specific services, create two custom policies and specify the scope respectively as **Global services** and **Project-level services**.

7. Select **Visual editor**.

8. In the **Policy Content** area, configure a custom policy.

   a. Select **Allow** or **Deny**.

   b. Select **Cloud service**.

      📖 NOTE

      Only one cloud service can be selected for each permission block. To configure permissions for multiple cloud services, click Add Permissions or switch to the **Creating a Custom Policy in the JSON View**.

   c. Select actions.

   d. (Optional) Select a resource type. For example, if you select **Specific**, you can click **Specify resource path** to specify the resource to be authorized.

e. (Optional) Add request conditions by specifying condition keys, operators, and values.

Table 5-1 Criterion

Name	Description
Condition Key	A key in the Condition element of a statement. There are global and service-level condition keys. ● Global-level condition key: The prefix is g:, which is applicable to all operations, as shown in **Table 5-2**. ● Project-level condition key: The prefix is the abbreviation of a service, for example, dns:. This key applies only to the operations of the corresponding service.
Operator	Used together with a condition key to form a complete condition statement.
Value	Used together with a condition key and an operator that requires a keyword, to form a complete condition statement.

Table 5-2 Global request condition

Global condition keys	Type	Description
g:CurrentTime	Time	Time when an authentication request is received. The time is in ISO 8601 format, for example, 2012-11-11T23:59:59Z.
g:DomainName	String	Account name
g:MFAPresent	Boolean	Whether to use multi-factor authentication (MFA) to obtain a token
g:MFAAge	Value	Validity period of the token obtained through MFA. This condition must be used together with g:MFAPresent.
g:ProjectName	String	Project name

Global condition keys	Type	Description
g:ServiceName	String	Service name
g:UserId	String	IAM user ID
g:UserName	String	IAM username

9. (Optional) Switch to the JSON view. Then you can modify the policy content in the JSON structure.

    ◻ NOTE

    If the JSON structure is wrong after modification, check the content, or click **Reset** to cancel the modification

10. (Optional) To add another permission block for the policy, click Add Permissions. Alternatively, click the plus (+) icon on the right of an existing permission block to clone its permissions.

11. (Optional) Describe the policy.

12. Click **OK**. The custom policy is created.

13. Assign the policy to a user group so that users in the group can inherit the permissions of the policy by referring to **Creating a User and Granting DNS Permissions**.

Creating a Custom Policy in the JSON View

1. Log in to the management console.

2. On the management console, hover over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.

3. In the left navigation pane, choose Permissions.

4. Click **Create Custom Policy**.

    The **Create Custom Policy** page is displayed.

5. Enter a policy name.

6. Select a scope in which the policy will take effect based on the type of services to be set in this policy.

    –   **Global services**: Select this option if the services to which the policy is related are available for all regions once deployed. When creating custom policies for globally deployed services, specify the scope as **Global services**. Custom policies of this scope must be attached to user groups in the Global service region.

    –   **Project-level services**: Select this option if the services to which the policy is related are deployed in specific regions. When creating custom policies for regionally deployed services, specify the scope as **Project-level services**. Custom policies of this scope must be attached to user groups in specific regions except the Global service region.

Select **Project-level services** here.

📖 NOTE

> A custom policy can contain actions of multiple services that are all globally available or all deployed only in specific projects. To define permissions required for accessing both globally available and project-specific services, create two custom policies and specify the scope respectively as **Global services** and **Project-level services**.

7. Select **JSON**.

8. (Optional) Click **Select Existing Policy**, and select a policy to use it as template, such as **DNS FullAccess**.

9. Click **OK**.

10. Modify the statements in the template.

   – **Effect**: Enter **Allow** or **Deny**.

   – **Action**: Enter the actions listed in the DNS API actions table, for example, dns:zone:create.

   📖 NOTE

   > The **Version** value of a custom policy must be **1.1**.

11. (Optional) Describe the policy.

12. Click **OK**. If the policy list is displayed, the policy is created successfully. If a message indicating incorrect policy content is displayed, modify the policy.

13. Assign the policy to a user group so that users in the group can inherit the permissions of the policy by referring to **Creating a User and Granting DNS Permissions**.

6 Key Operations Recorded by CTS

6.1 DNS Operations Recorded by CTS

CTS is interconnected with the DNS service to record 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 6-1 lists the DNS operations that will be recorded by CTS.

◯ NOTE

> **Table 6-1** lists DNS operations at the region level. Traces of these operations are displayed in the regions where the operations are performed.

Table 6-1 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 in 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

Operation	Resource Type	Trace Name
Disassociating a VPC from a private zone	privateZone	disassociateRouter

6.2 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. Click **Service List** and select **Cloud Trace Service** under **Management & Deployment**.

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.

7 Quota Adjustment

What Is Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number and capacity of resources available to users, for example, the maximum number of zones or record sets that you can create.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.

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

3. In the upper right corner of the page, click   .

    The **Service Quota** page is displayed.

4. 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, call the hotline or send an email to the customer service mailbox. Customer service personnel will timely process your request for quota adjustment and inform you of the real-time progress by making a call or sending an email.

Before dialing the hotline number or sending an email, make sure that the following information has been obtained:

-   Account name, project name, and project ID, which can be obtained by performing the following operations:

    Log in to the management console using the cloud account, click the username in the upper right corner, select **My Credentials** from the drop-down list, and obtain the account name, project name, and project ID on the **My Credentials** page.

- Quota information, which includes:
  - Service name
  - Quota type
  - Required quota

Learn how to obtain the service hotline and email address.

8 FAQs

8.1 DNS Overview

8.1.1 Will I Be Billed for the DNS Service?

Yes.

The DNS service is charged in two parts:

- Zone: charged based on how long the domain name is managed
- Record set: charged based on the domain resolution counts

8.1.2 How Many Zones/Record Sets Can I Create?

By default, you can create a maximum of 50 private zones and 500 record sets.

If the quotas do not meet your service requirements, you can contact customer service for an increase.

8.1.3 Are Wildcard DNS Record Sets Supported?

Yes.

You can use an asterisk (*) as the host name in a domain name to create a wildcard record set. For more details, see RFC 4592.

Currently, you can create a wildcard DNS record set of the A, AAAA, MX, CNAME, TXT, or SRV types.

8.1.4 How Are Zones Queried to Resolve a Domain Name?

When a domain name request is initiated, the domain name is first queried in the zone of a subdomain of the domain name.

- If the zone created for the subdomain exists, the system returns the result from the zone configuration file.
- Otherwise, the system queries the domain name from the zone configuration file of a higher-level domain name.

For example, you have created a zone for example.com and added an A record set for www.example.com. You have also created a zone for www.example.com but have not added an A record set for it.

In this case, if a visitor tries to access www.example.com, the domain name is first queried in the configuration file of zone www.example.com. However, because you have not added an A record set in the zone, no result will be returned.

8.1.5 Why Is the Email Address Format Changed in the SOA Record?

When you create a zone, we strongly recommend you specify **HOSTMASTER@***Domain name* as the email address.

After the zone is created, the email you specified is displayed in the SOA record set of the zone. Because the "@" sign in the SOA record set has other meanings, the system replaces @ in the email address with a dot (.). If a dot already exists before the @ sign, the system includes a backslash (\) before the dot. However, emails are still sent to the email address you specified. For more details, see RFC 1035.

Take **test.hostmaster@example.com** as an example.

If you have specified **test.hostmaster@example.com** when creating the zone, the email address displayed in the SOA record set is **test\.hostmaster.example.com**.

8.2 Private Zones

8.2.1 How Can I Configure a PTR Record for the Private IP Address of an ECS?

PTR records enable visitors to query domain names based on IP addresses.

If you want to set PTR records for an ECS, create a private zone and create PTR records in the zone.

📖 **NOTE**

The domain name in a PTR record is specified in the *x.x.x.x*.**in-addr.arpa** format. **in-addr.arpa** is the domain name suffix for reverse resolution.

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

In this case, create a private zone **192.in-addr.arpa** and add a PTR record **10.1.168.192.in-addr.arpa**.

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, 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 the parameters based on **Table 8-1**.

Table 8-1 Parameters for creating a private zone

Parameter	Description	Example Value
Name	Domain name Set the domain name suffix to **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 It is recommended that you set the email address to **HOSTMASTER@*Domain name***. For more information about the email address, see **Why Is 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. Before you set this parameter, create an enterprise project by referring to **Creating an Enterprise Project**.	default
Tags	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a zone. For details about tag key and value requirements, see **Table 8-2**.	example_key1 example_value1

Parameter	Description	Example Value
Description	(Optional) Supplementary information about the zone You can enter a maximum of 255 characters.	This is a private zone.

Table 8-2 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.	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters.	example_value1

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

   View the created private zone.

   📖 NOTE

   Click the zone name to view detailed zone information. You can view SOA and NS record sets created by the system.

   ● The SOA record set defines the DNS server that is the authoritative information source for a particular domain name.
   ● The NS record set defines authoritative DNS servers for a zone.

Adding a PTR Record

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

   The **Record Sets** page is displayed.
2. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
3. Set the parameters based on **Table 8-3**.

Table 8-3 Parameters for adding a PTR record

Parameter	Description	Example Value
Name	IP address in the PTR record (typed in reverse order)	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 name is **192.in-addr.arpa**, enter **10.1.168** in the box. ● If the private zone name is **1.168.192.in-addr.arpa**, enter **10** in the box.
Type	Type of the record set	PTR – Map IP addresses to domains
TTL (s)	Cache duration of the record set, in seconds	The default value is **300**, which is, 5 minutes.
Value	Domain name mapped to the IP address You can enter only one name.	mail.example.com
Tags	(Optional) Identifier of a resource 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 8-2**.	example_key1 example_value1
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** page.

   View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

A Change History

Released On	Description
2020-02-26	This issue is the first official release.