Domain Name Service

User Guide

Date   **2022-04-01**

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

  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 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 the VPCs without having to connect to the Internet. These ECSs can also access cloud services, such as OBS and SMN, over a private network.

Figure 1-1 shows how a private domain name is resolved by a private DNS server.
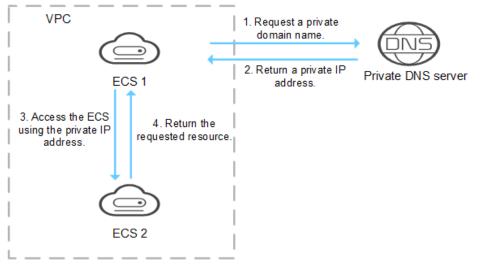
Figure 1-1 Process for resolving a private domain name

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 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 1-2 illustrates such use of private domain name resolution.
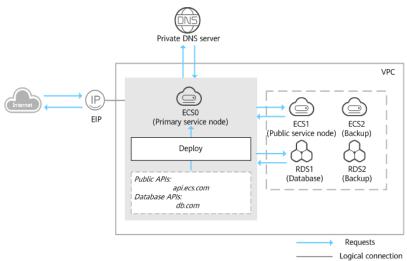
Figure 1-2 Configuring private DNS for cloud servers

The ECSs and RDS instances are in the same VPC.

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

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

Now assume that you have configured private zones for the ECSs and have included their private names in the code. If ECS1 becomes faulty, you only need to change the DNS records to direct traffic to ECS2. Services are not interrupted, and you do not need to publish the website again.

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.
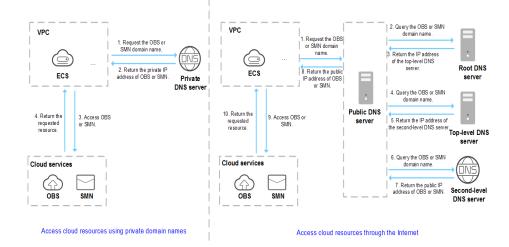
  Figure 1-3 shows the process for resolving a domain name when an ECS accesses cloud services such as OBS and SMN.
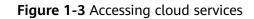
  Requests are routed over the Internet, resulting in an increase in network latency.

- 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 1-3** shows the process.

Figure 1-3 Accessing cloud services

1.3 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 part 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:

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

Table 1-1 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 1-2 lists the common operations supported by each DNS system policy or role. Choose proper system policies according to this table.

Table 1-2 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	√
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	√

Related References

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

1.4 Integration with Other Services

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

Table 1-3 DNS and other services

Related Service	Description	Reference
Virtual Private Cloud (VPC)	Create VPCs for the DNS service.	**Routing Traffic Within VPCs**

1.5 Product Concepts

1.5.1 Domain Name Format and DNS Hierarchy

A valid domain name meets the following requirements:

- A domain name is segmented using periods (.) 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 period 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.

1.5.2 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	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.

Type	Usage
TXT	Creates text records for domain names. 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.
NS	Delegates subdomains to other name servers. This type of record set is created by default and cannot be added manually.
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

PTR records translate private IP addresses into private domain names.

Figure 1-5 Reverse resolution on a private network

Helpful Links

For details, see **Overview**.

1.5.3 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 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. Obtain the regions and endpoints from the administrator.

1.5.4 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.

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 Routing Traffic Within VPCs

Scenarios

If you have deployed ECSs and other cloud services, 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.

The following are operations for you to create a private zone and add an A record set to it.

Prerequisites

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

Procedure

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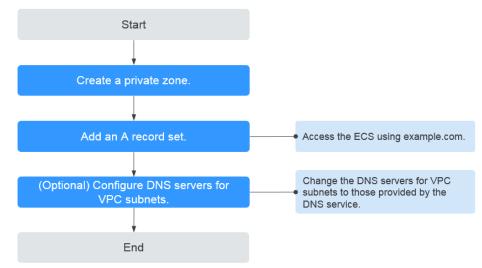
Figure 2-1 Process for configuring a private zone

> **NOTE**
>
> To ensure that the private domain name can be resolved in a VPC, verify that the DNS server addresses for the VPC subnet are those provided by the DNS service. For DNS server addresses in each region, see **What Are the Private DNS Servers Provided by the DNS Service?** If the DNS server addresses are not those provided by the DNS service, change them.
>
> You can view or change the DNS server addresses for the VPC subnet by performing the operations in **Step 3. (Optional) Configure DNS Server Addresses for the VPC Subnet**.

Step 1. 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 zone details. You can view SOA and NS record sets automatically generated 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.

Step 2. 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. Configure the parameters as follows:

   - **Name**: Leave this parameter blank. The system automatically considers example.com to be 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 settings 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**.

Step 3. (Optional) Configure DNS Server Addresses for the VPC Subnet

To ensure that the private domain name can be resolved in a VPC, verify that the DNS server addresses for the VPC subnet are those provided by the DNS service. For DNS server addresses in each region, see **What Are the Private DNS Servers 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, 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 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 **Modifying a Subnet**.

3 Private Zone

3.1 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.

This chapter describes how to create and manage private zones.

Table 3-1 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 a maximum of 50 private zones. - Private domain names must meet the following requirements: - Domain name labels are separated by period (.), 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 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	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.

3.2 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, 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 your other cloud resources are deployed, such as cloud servers. Otherwise, the domain name cannot be resolved.	-
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
Tag	(Optional) Identifier of the domain name. 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

Parameter	Description	Example Value
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. • Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1
Value	• Cannot be left blank. • Can contain a maximum of 43 characters. • Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	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 zone details. You can view SOA and NS record sets automatically generated 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 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 email address of the domain name administrator and description of the private zone.

📖 **NOTE**

For more information about the email address, 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, 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**.

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. Locate the private zone you want to view and click ∨ before the zone name to view its details.

3.4 Managing Private Zone Tags

Scenarios

A tag is the identifier of a private zone. Adding tags to private zones helps you identify and manage your private zones. You can add tags when creating a private zone or add tags to existing private zones. Up to 10 tags can be added to a private zone.

A tag consists of a key and value pair. **Table 3-4** lists the tag key and value requirements.

Table 3-4 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. - Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1
Value	- Cannot be left blank. - Can contain a maximum of 43 characters. - Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_value1

Procedure

In the private zone list, search for the private zone by tag key or value.

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 upper right corner of the private zone list, click **Search by Tag**.

6. Enter the tag key and value of the private zones you want to query.

   Both the tag key and value must be specified. The system automatically displays the private zones you are looking for if both the tag key and value are matched.

7. Click **+** to add more tag keys and values.

   You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for private zones, the private zones containing all specified tags will be displayed.

8. Click **Search**.

   The system searches for private zones by tag key and value.

In the private zone details area, add, delete, modify, and query tags.

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. On the **Private Zones** page, click ⌄ to view details about the private zone.

   The details of the private zone are displayed.

   Figure 3-1 Private zone details

6. In the **Tags** area, query, add, modify, or delete tags.
   – Query tags.

In the **Tags** area, view details about tags, including the number of tags and the key and value of each tag.

- Add a tag.

  Click **Add Tag** in the upper left corner. In the displayed **Add Tag** dialog box, enter the tag key and value, and click **OK**.

- Modify a tag.

  Locate the row that contains the tag you want to edit and click **Edit** in the **Operation** column. In the **Edit Tag** dialog box, change the tag value and click **OK**.

- Delete a tag.

  Locate the row that contains the tag to be deleted and click **Delete** in the **Operation** column. In the displayed **Delete Tag** dialog box, click **Yes**.

3.5 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, such as cloud servers. 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**.

3.6 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, 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	Constraints
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 for 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 or delete SOA and NS record sets automatically generated by the system.
Creating 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 4-1 shows the process for configuring a record set on the DNS console.
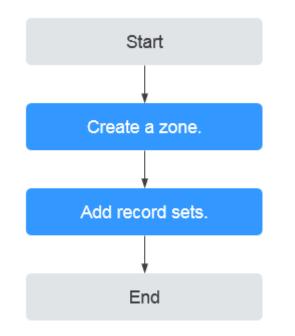
Figure 4-1 Process for configuring a record set

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.
NS	Delegates subdomains to other name servers. This type of record set is created by default and cannot be added manually.

Type	Description
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
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

Record Set Type	Value	Example
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"
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. In some cases, you may need to set the record set name to the at sign (@). However, the at sign is not supported. Leave the **Name** 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 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 **300** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	The default value is 300s, which is, 5 minutes.
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
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. This parameter is displayed when you expand **More Settings**. For details about tag key and value requirements, see **Table 4-5**.	example_key1 example_value1

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

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. • Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1
Value	• Cannot be left blank. • Can contain a maximum of 43 characters. • Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	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 details about how to configure A record sets, see **Routing Traffic Within VPCs**.

4.3.2 Adding an AAAA Record Set

Scenarios

If you want your 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 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. In some cases, you may need to set the record set name to the at sign (@). However, the at sign is not supported. Leave the **Name** 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 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.	AAAA – Map domains to IPv6 addresses

Parameter	Description	Example Value
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **300** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	The default value is 300s, 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.	ff03:0db8:85a3:0:0:8a2e:0370:7334
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. This parameter is displayed when you expand **More Settings**. For details about tag key and value requirements, see **Table 4-7**.	example_key1 example_value1
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. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	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**.

4.3.3 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.	Left blank
	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. In some cases, you may need to set the record set name to the at sign (@). However, the at sign is not supported. Leave the **Name** 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 an email server.	
	● *****: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com.	
Type	Type of the record set	CNAME – Map one domain to another
	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.	
TTL (s)	Cache duration of the record set on a local DNS server, in seconds.	The default value is 300s, which is, 5 minutes.
	The value ranges from **300** to **2147483647**, and the default is **300**.	
	If your service address changes frequently, set TTL to a smaller value.	
Value	Domain name alias. You can enter only one domain name.	webserver01.example.com
Tag	(Optional) Identifier of the record set.	example_key1
	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 expand **More Settings**.	example_value 1
	For details about tag key and value requirements, see **Table 4-9**.	

Parameter	Description	Example Value
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. • Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1
Value	• Cannot be left blank. • Can contain a maximum of 43 characters. • Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	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**.

4.3.4 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 **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

Paramete r	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. In some cases, you may need to set the record set name to the at sign (@). However, the at sign is not supported. Leave the **Name** 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 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 **300** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	The default value is 300s, which is, 5 minutes.

Parameter	Description	Example Value
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
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. This parameter is displayed when you expand **More Settings**. For details about tag key and value requirements, see **Table 4-11**.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	-

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. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	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**.

4.3.5 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. In some cases, you may need to set the record set name to the at sign (@). However, the at sign is not supported. Leave the **Name** 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 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 **300** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	The default value is 300s, 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"
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. This parameter is displayed when you expand **More 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. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1

Paramete r	Requirements	Example Value
Value	- Cannot be left blank. - Can contain a maximum of 43 characters. - Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	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**.

4.3.6 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 **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
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **300** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	The default value is 300s, 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

Parameter	Description	Example Value
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. This parameter is displayed when you expand **More 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

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 characters. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	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**.

4.3.7 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 **Record Set Types and Configuration Rules**.

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

Parameter	Description	Example Value
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **300** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	The default value is 300s, which is, 5 minutes.
Value	Private domain name mapped to the private IP address. You can enter only one domain name.	host.example.com.
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. This parameter is displayed when you expand **More Settings**. For details about tag key and value requirements, see **Table 4-17**.	example_key1 example_value1
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. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	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, see **How Can I Configure a PTR Record to Map the IP Address of an ECS to a Domain Name?**

4.4 Managing Record Sets

Scenarios

You can modify, 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 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**.

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 Managing Record Set Tags

Scenarios

A tag is the identifier of a record set. Adding tags to record sets helps you identify and manage your record sets. You can add tags when adding a record set or add tags to an existing record set. Up to 10 tags can be added to a record set.

A tag consists of a key and value pair. **Table 4-18** lists the tag key and value requirements.

Table 4-18 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. - Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1

Parameter	Requirements	Example Value
Value	- Cannot be left blank. - Can contain a maximum of 43 characters. - Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_value1

Procedure

In the record set list, search for record sets by tag key or value.

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. Click the private zone.
   The **Record Sets** page is displayed.
6. In the upper right corner of the record set list, click **Search by Tag**.
7. Enter the tag key and value of the record sets you want to query.
   Both the tag key and value must be specified. The system automatically displays the record sets you are looking for if both the tag key and value are matched.
8. Click **+** to add more tag keys and values.
   You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for record sets, the record sets containing all specified tags will be displayed.
9. Click **Search**.
   The system searches for the record sets by tag key and value.

In the record set details area, add, delete, modify, and query tags.

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. Click the private zone.
   The **Record Sets** page is displayed.
6. On the **Record Sets** page, click ⌄ to view its details.
   The details of the record set are displayed.

Figure 4-2 Record set details

7. In the **Tags** area, query, add, modify, or delete tags.

   – Query tags.

   In the **Tags** area, view details about tags, including the number of tags and the key and value of each tag.

   – Add a tag.

   Click **Add Tag** in the upper left corner. In the displayed **Add Tag** dialog box, enter the tag key and value, and click **OK**.

   – Modify a tag.

   Locate the row that contains the tag you want to edit and click **Edit** in the **Operation** column. In the **Edit Tag** dialog box, change the tag value and click **OK**.

   – Delete a tag.

   Locate the row that contains the tag to be deleted and click **Delete** in the **Operation** column. In the displayed **Delete Tag** dialog box, click **Yes**.

4.6 Creating 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 matching is used.

📖 **NOTE**

Exact matching has a higher priority than fuzzy matching.

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 **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. Configure the parameters based on **Table 4-19**.

Table 4-19 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 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 **300** to **2147483647**, and the default is **300**. If your service address changes frequently, set TTL to a smaller value.	The default value is 300s, 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

Paramete r	Description	Example Value
Tag	(Optional) Identifier of the record set.	example_key1
	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 expand **More Settings**.	example_value1
	For details about tag key and value requirements, see **Table 4-20**.	
Descriptio n	(Optional) Supplementary information about the record set.	This is a wildcard DNS record set.
	You can enter a maximum of 255 characters.	

Table 4-20 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. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	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**.

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.

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

The following describes the procedure for granting permissions (see **Figure 5-1**).

Prerequisites

Learn about the permissions.
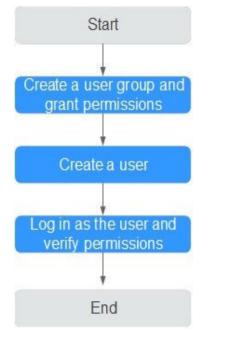
Process Flow

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 in and 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.

Some examples of common custom DNS policies are provided.

Creating a Custom Policy in the Visual Editor

1. Log in to the management console.
2. Choose **Management & Deployment** > **Identity and Access Management**.

   The **Identity and Access Management** page is displayed.
3. In the left navigation pane, choose Policies.
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 applies 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
g:ServiceName	String	Service name

Global condition keys	Type	Description
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. Choose **Management & Deployment** > **Identity and Access Management**.

The **Identity and Access Management** page is displayed.

3. In the left navigation pane, choose Policies.

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 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 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. 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, contact the administrator.

Before contacting the administrator, make sure that the following information has been obtained:

- Domain 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 domain name, project name, and project ID on the **My Credentials** page.

- Quota information, which includes:

- Service name
- Quota type
- Required quota

7 FAQs

7.1 DNS Overview

7.1.1 Will I Be Billed for the DNS Service?

DNS is free. You can use the DNS service free of charge.

7.1.2 How Many Zones and Record Sets Can I Create?

By default, you can use an account to create up to 50 private zones and 500 record sets.

If the quotas do not meet your service requirements, contact the administrator to request an increased quota.

7.1.3 What Are the Private DNS Servers Provided by the DNS Service?

Private DNS servers are used in VPCs to:

- Resolve private domain names and internal domain names of cloud services.
- Forward domain name requests to public DNS servers.

You can use private DNS servers provided by the DNS service to:

- Resolve private domain names used in VPCs.
- Access cloud services such as OBS and SMN.
- Allow ECSs without EIPs to access the Internet.

Table 7-1 lists private DNS server addresses provided by the DNS service in different regions.

Table 7-1 Private DNS server addresses

Region	Private DNS server addresses
eu-ch2	100.125.4.25
	100.125.64.24

7.1.4 Does DNS Support Wildcard Entries?

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, and SRV.

7.1.5 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 named **example.com** and added an A record set to it, with the **Name** field set to **www**, and you have also created another zone named **www.example.com** but have not added an A record set to this zone.

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

7.1.6 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 period (.) and includes a backslash (\) before the period in the label before the at sign, but emails are still sent to the email address you specify. 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**.

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

DNS cannot point a domain name to an IP address with a specific port (*Server IP address*:*Port number*).

7.2 Private Zones

7.2.1 How Can I Configure a PTR Record to Map the IP Address of an ECS to a Domain Name?

PTR records enable 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 create a PTR record in the zone.

☐ NOTE

The domain name in a 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 in the PTR record must be **10.1.168.192.in-addr.arpa**.

In this case, you must create a private zone named **192.in-addr.arpa** and add a PTR record with its value set to **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. Configure the parameters based on **Table 7-2**.

   Table 7-2 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

Parameter	Description	Example Value
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
Tag	(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 7-3**.	example_key1 example_value1
Description	(Optional) Supplementary information about the zone You can enter a maximum of 255 characters.	This is a private zone.

Table 7-3 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. • Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_key1

Paramete r	Requirements	Example Value
Value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), at signs (@), and underscores (_).	example_value 1

7. Click **OK**.

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

   View the created private zone.

   📖 **NOTE**

   Click the zone name to view zone details. You can view SOA and NS record sets automatically generated 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.

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. Configure the parameters based on **Table 7-4**.

Table 7-4 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 300s, which is, 5 minutes.
Value	Domain name mapped to the IP address. You can enter only one name.	mail.example.com
Tag	(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 7-3**.	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
2022-04-01	This issue incorporates the following changes: Modified the following content: Modified the region name in **What Are the Private DNS Servers Provided by the DNS Service?**.
2022-03-24	This issue incorporates the following changes: Modified the following content: ● Optimized the scenario description of changing the DNS server addresses for a VPC subnet in **Routing Traffic Within VPCs**. ● Changed the maximum number of tags allowed to be added to 10 in **Managing Private Zone Tags** and **Managing Record Set Tags**. ● Changed the record set types that support wildcard DNS resolution in **Overview**, **Creating a Wildcard DNS Record Set**, and **Does DNS Support Wildcard Entries?**

Released On	Description
2022-02-25	This issue incorporates the following changes: Modified the following content: • Deleted the description of public zones in and added some reference links in **Permissions Management**. • Modified the tag specifications. • Added the description of the NS record set in section **Record Set Types and Configuration Rules**. • Changed the value range of TTL to 300–21447483647. • Modified the link in **Adding a PTR Record**. • Deleted the description of enabling and disabling record sets in **Managing Record Sets**. Added the following sections: • **Managing Private Zone Tags** • **Managing Record Set Tags**
2021-10-30	This issue is the first official release.