# Domain Name Service

# User Guide

**Issue** 01

**Date** 2024-12-24

HUAWEI

**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**

### Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

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

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

## Huawei Cloud Computing Technologies Co., Ltd.

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

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

# Contents



# 1 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 create custom 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 much faster.

- Easy access to cloud resources

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

- Isolation of core data

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

### Accessing the DNS Service

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

- Management console

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

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*.

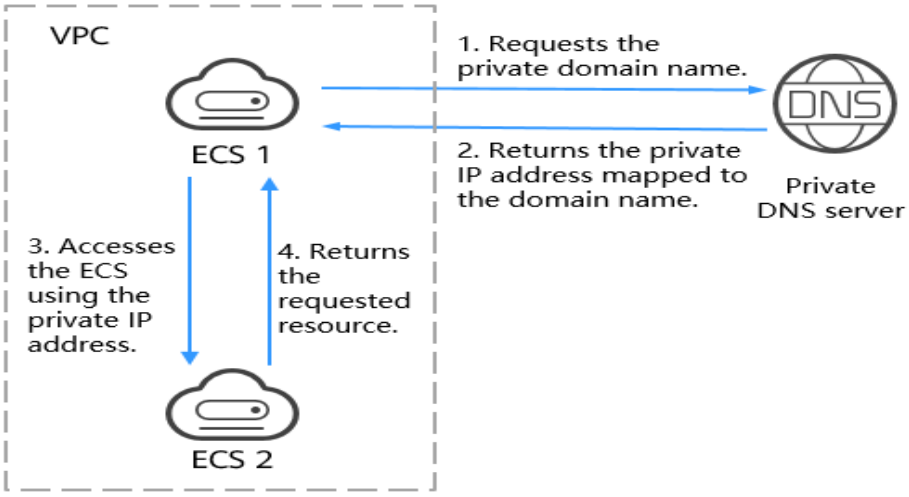
# 1.2 Private Domain Name Resolution

## 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 zones, ECSs within a VPC can communicate with each other using private domain names. 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 to access a private domain name, the private DNS server directly returns a private IP address mapped to the domain name.

Private zones allow you to:

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

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" in "Getting Started" 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.

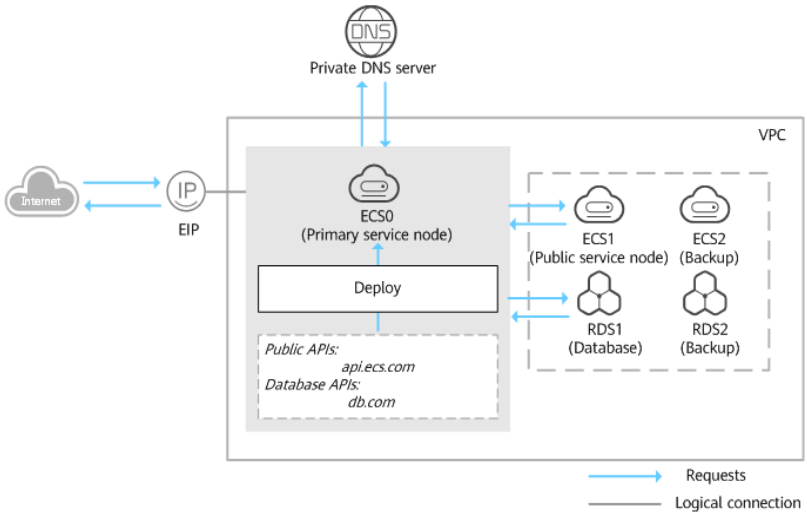
These servers are in the same VPC and communicate with each other using private IP addresses that are coded into internal APIs called among the servers. If one of these servers is replaced, its private IP address changes. As a result, you need to change this IP address in the APIs and re-publish the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

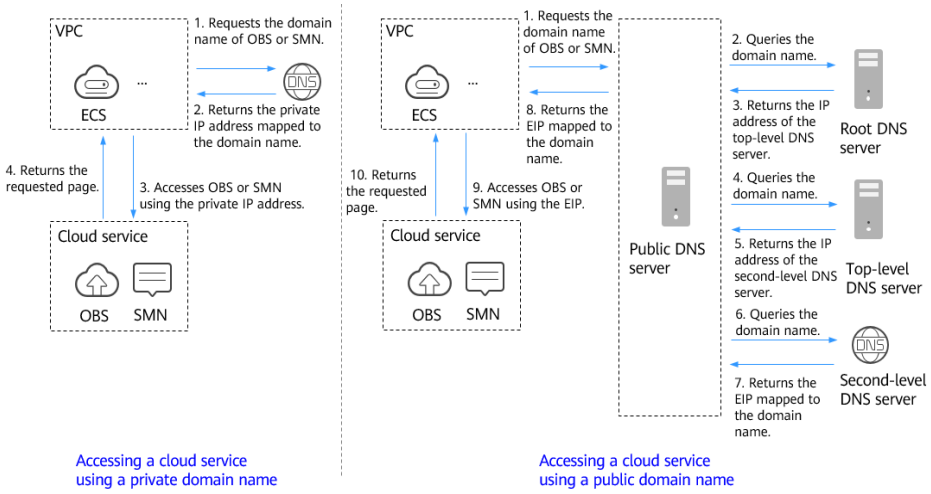
  Requests are routed over the Internet, resulting in high network latency and poor user experience.
- If a private DNS server is configured for the subnet, the private DNS server directly processes the requests to access cloud services.

  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

If you need to assign different permissions to personnel in your enterprise to access your DNS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely access your cloud resources.

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

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

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

For more information about IAM, see IAM Service Overview.

## DNS Permissions

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

DNS resources include the following:

- Private zones: project-level resources
- PTR records: project-level resources

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

When you set **Scope** to **Region-specific projects** and select the specified projects in the specified regions, the users only have permissions for DNS in the selected projects. If you set **Scope** to **All resources**, the users have permissions for DNS in all region-specific projects. When accessing DNS, the users need to switch to the authorized region.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Cloud services depend on each other. When you grant permissions using roles, you also need to attach dependent roles. Roles are not ideal for fine-grained authorization and least privilege access.
- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permissions to manage DNS resources of a certain type. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by DNS, see "Permissions and Supported Actions" in the *Domain Name Service API Reference*.

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

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

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

**Table 1-2** lists common operations supported by system-defined permissions for DNS.

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

| Operation | DNS FullAccess | DNS ReadOnlyAccess | DNS Administrator |
|---|---|---|---|
| Creating a private zone | Supported | Not supported | Supported |
| Viewing a private zone | Supported | Supported | Supported |
| Modifying a private zone | Supported | Not supported | Supported |
| Deleting a private zone | Supported | Not supported | Supported |
| Deleting private zones in batches | Supported | Not supported | Supported |
| Associating a VPC with a private zone | Supported | Not supported | Supported |
| Disassociating a VPC from a private zone | Supported | Not supported | Supported |
| Adding a record set | Supported | Not supported | Supported |
| Viewing a record set | Supported | Supported | Supported |
| Modify a record set | Supported | Not supported | Supported |
| Deleting a record set | Supported | Not supported | Supported |
| Delete record sets in batches | Supported | Not supported | Supported |

### Related References

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

## 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) | DNS can resolve private domain names that are used for network connections within VPCs. | **Routing Traffic Within VPCs** in the **Before You Start** |

# 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 period)
- 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 provides information about a domain name, including the IP addresses associated with and how to handle requests for the domain name and its subdomains.

If you have created a zone on the DNS console, you can add record sets to define how you want to route traffic for the domain name or its subdomains.

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

**Table 1-4** Record set usages

| Type | Description |
| --- | --- |
| A | Maps domains to IPv4 addresses. |
| CNAME | Maps one domain name to another domain name or multiple domain names to one domain name. |
| MX | Maps domain names to email servers. |
| AAAA | Maps domain names to IPv6 addresses. |

| Type | Description |
| --- | --- |
| TXT | Creates text records for domain names. TXT record sets are usually used in the following scenarios:<br>• To record DKIM public keys to prevent email fraud.<br>• 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.<br>This type of record set is created by default and cannot be added manually. |
| SOA | Identifies the base information about a domain name. The SOA record set is automatically generated by the DNS service and cannot be added manually. |
| 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 about how to add and manage record sets, see **Record Set Management** in the **User Guide**.

# 1.5.3 Region and AZ

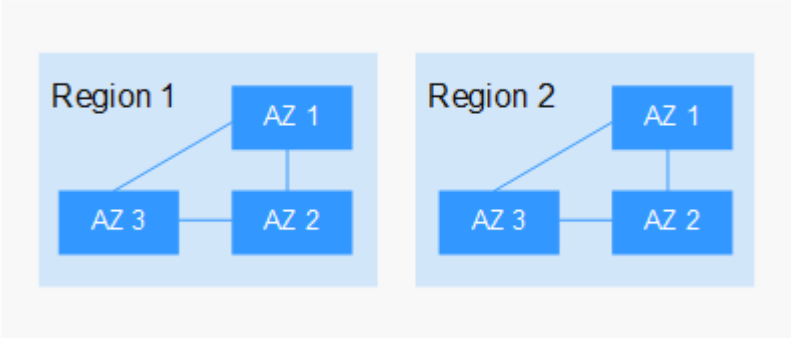
## Concept

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. For more details, see **Regions and Endpoints**.

# 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 and 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 Private Domain Name Resolution for ECSs

### Scenarios

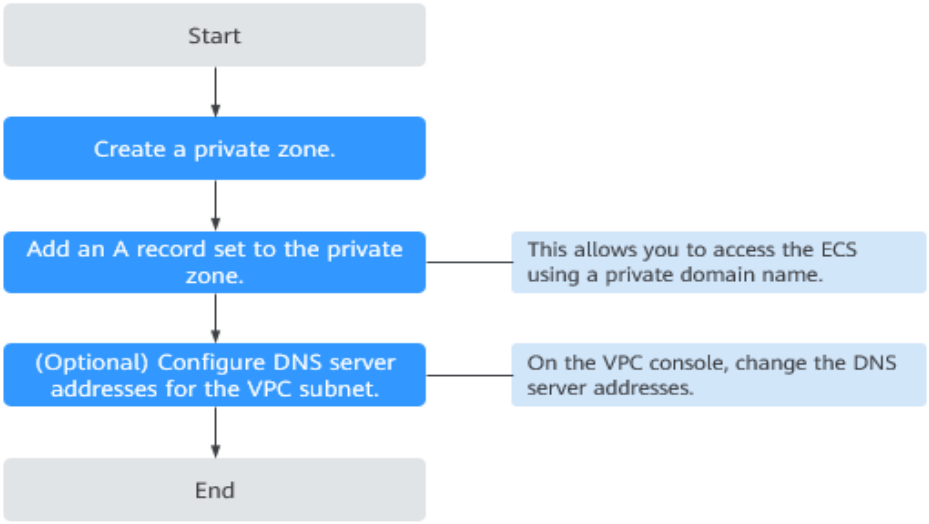
If you have deployed ECSs and other cloud services in a VPC, you can configure private domain names for the ECSs so that they can communicate with each other or access the cloud services over a private network.

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

### Procedure

Figure 2-1 shows the process of configuring a private domain name for an ECS.

**Figure 2-1** Configuring a private domain name for an ECS



NOTE

To make the private zone and its record sets take effect in a VPC, ensure that the VPC subnets use the private DNS server addresses provided by the DNS service.

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

## Step 1: Create a Private Zone

Before using a private domain name (for example, example.com) to access an ECS, you need to create a private zone.

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

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

   The **Private Zones** page is displayed.
4. Click  on the upper left and select the desired region and project.
5. In the upper right corner of the page, click **Create Private Zone**.
6. On the **Create Private Zone** page, configure parameters as prompted. For details, see **Creating a Private Zone**.
7. Click **OK**.
8. Switch back to the **Private Zones** page.

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

   NOTE

   You can click the domain name to view SOA and NS record sets automatically added to the zone.

   - The SOA record set includes administrative information about your zone, as defined by the Domain Name System (DNS).
   - The NS record set defines the authoritative DNS servers for the domain name.

## Step 2: Add an A Record Set

Add an A record set for the created private zone.

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

   The **Record Sets** tab is displayed.
2. In the upper right corner of the page, click **Add Record Set**.
3. Configure the parameters as follows:
   - **Name**: Leave this parameter blank. This is a record set for the domain name, which is example.com.
   - **Type**: Retain the default setting **A – Map domains to IPv4 addresses**.
   - **Value**: Enter the private IP address of the ECS.

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

5. Switch back to the **Record Sets** tab.
   The added record set is in the **Normal** state.

## Step 3: Change the DNS Servers for the VPC Subnet

To make the private zone and its record sets take effect in a VPC, ensure that the VPC subnets use the private DNS server addresses provided by the DNS service. If the DNS server addresses are not those provided by the DNS service, change them.

**Step 1** View the private DNS server addresses for the VPC subnet.

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click  on the upper left and select the desired region and project.
5. In the private zone list, locate the private zone and click the domain name.
   View the private DNS server addresses for the VPC subnet on the top of the record set list.
6. Check whether the private DNS server addresses are the same as those provided by the DNS service. If they are different, go to **Step 2**.

**Step 2** Change the private DNS server addresses for the VPC subnet.

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

**----End**

# 3 Private Zones

## 3.1 Private Zone 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 for each domain name and associate VPCs with the private zone.

**Table 3-1** describes the operations that you can perform on 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.<br>• Each account can create up to 50 private zones.<br>• Private domain names must meet the following requirements:<br>– Domain name labels are separated by period (.), and each label does not exceed 63 characters.<br>– A domain name label can contain letters, digits, and hyphens (-) and cannot start or end with a hyphen.<br>– The total length of a domain name cannot exceed 254 characters. |
| **Managing Private Zones** | Modify, delete, and view private zones. | • The domain name of a created private zone cannot be modified.<br>• If a private zone is deleted, all its record sets will also be deleted. |
| **Associating a VPC with a Private Zone** | Associate a VPC with a private zone. | • You can only associate VPCs that you have created using your own account.<br>• 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.<br>• 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 on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click  on the upper left and select the desired region and project.
5. In the upper right corner of the page, click **Create Private Zone**.
6. Configure the parameters.
   Table 3-2 describes the parameters.

**Table 3-2** Parameters for creating a private zone

| Parameter | Description | Example Value |
| --- | --- | --- |
| Domain Name | Domain name you have planned for the ECS.<br>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.<br>**NOTE**<br>This VPC must be the same as the VPC where your other cloud resources are deployed. If the VPC is different, the domain name cannot be resolved. | - |
| Email | (Optional) Email address of the administrator managing the private zone.<br>Recommended email address: **HOSTMASTER@*Domain name***<br>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 zone.<br>Each tag contains a key and a value. You can add up to 10 tags to a zone.<br>For details about tag key and value requirements, see **Table 3-3**. | example_key1<br>example_value1 |
| Description | (Optional) Supplementary information about the zone.<br>The description can contain no more than 255 characters. | This is a zone example. |

**Table 3-3** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value1 |

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

   You can view the created private zone in the zone list.
9. Click the domain name to add record sets.

   On the **Record Sets** tab, click **Add Record Set**. For details about the parameters, see **Record Set Overview**.

   NOTE

   You can click the domain name to view SOA and NS record sets automatically added to the zone.

   - The SOA record set includes administrative information about your zone, as defined by the Domain Name System (DNS).
   - The NS record set defines the authoritative DNS servers for the domain name.

## Follow-up Operations

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

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

# 3.3 Managing Private Zones

## Scenarios

You can modify or delete private zones, or view their details.

## Modifying a Private Zone

Change the domain name administrator's email address and description for a 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 on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click on the upper left and select the desired region and project.
5. Locate the private zone you want to modify and choose **More** > **Modify** in the **Operation** column.
   The **Modify Private Zone** dialog box is displayed.
6. Modify the private zone.
7. Click **OK**.

## Deleting a Private Zone

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

NOTICE

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

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click on the upper left and select the desired region and project.
5. Locate the private zone you want to delete and choose **More** > **Delete** in the **Operation** column.
   The **Delete Private Zone** dialog box is displayed.
6. In the displayed dialog box, 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 on the upper left and select the desired region and project.
5. In the private zone list, click the name of the private zone 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 be resolved within this VPC.

NOTE

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

## Procedure

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click on the upper left and select the desired region and project.
5. Locate the private zone with which you want to associate the VPC and click **Associate VPC** in the **Operation** column.
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 in the **Associated VPC** column.

# 3.5 Disassociating a VPC from a Private Zone

## Scenarios

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

NOTE

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

## Procedure

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click  on the upper left 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 in the **Associated VPC** column, and click  on the right of the VPC.
6. In the **Disassociate VPC** dialog box, click **Yes**.

# 4 Record Sets

## 4.1 Record Set Overview

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

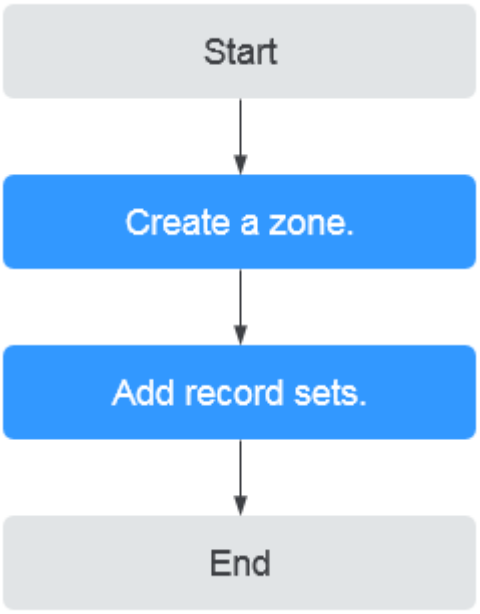
**Table 4-1** Record set management

| Operation | Scenario | Constraints |
| --- | --- | --- |
| **Adding Record Sets** | View record set types supported by the DNS service and their configuration rules, and configure record sets for a domain name.<br>For details, see **Table 4-2**. | • After a zone is created for a domain name, SOA and NS record sets are automatically created.<br>• Up to 500 record sets can be added by an account. |
| **Managing Record Sets** | Modify, delete, and view record sets. | • After a record set is added, its resolution line cannot be modified.<br>• You cannot modify or delete SOA and NS record sets automatically generated by the system. |
| **Configuring a Wildcard DNS Record Set** | Add a record set that matches all subdomains. | Wildcard DNS resolution does not support NS and SOA record sets. |

**Figure 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 Adding Record Sets

## 4.2.1 Record Set Types and Configuration Rules

### Record Set Types

Table 4-2 describes the record set types.

**Table 4-2** Record set types

| Record Set Type | Description | Value | Example |
| --- | --- | --- | --- |
| A | Maps domains to IPv4 addresses. | IPv4 addresses mapped to the domain name.<br>You can enter up to 50 values, each on a separate line. | 192.168.12.2<br>192.168.12.3 |
| CNAME | Maps one domain name to another domain name or multiple domain names to one domain name. | Domain name alias. You can enter only one domain name. | www.example.com |

| Record Set Type | Description | Value | Example |
| --- | --- | --- | --- |
| MX | Maps domain names to email servers. | Email server address<br>You can enter up to 50 values, each on a separate line.<br>The format is **[priority] [mail server host name]**.<br>Configuration rules:<br>• **priority**: priority for an email server to receive emails. A smaller value indicates a higher priority.<br>• **mail server host name**: domain name provided by the email service provider | 10 mailserver.example.com.<br>20 mailserver2.example.com. |
| AAAA | Maps domain names to IPv6 addresses. | IPv6 addresses mapped to the domain name.<br>You can enter up to 50 values, each on a separate line. | ff03:0db8:85a3:0:0:8a2e:0370:7334 |

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

| Record Set Type | Description | Value | Example |
| --- | --- | --- | --- |
| SRV | Records servers providing specific services. | Server address<br>You can enter up to 50 values, each on a separate line.<br>The value format is **[priority] [weight] [port number] [server address]**.<br>Configuration rules:<br>• The priority, weight, and port number range from 0 to 65535.<br>• A smaller value indicates a higher priority.<br>• A larger value indicates a larger weight.<br>• The server address is the domain name of the target server. Ensure that the domain name can be resolved.<br>**NOTE**<br>If the record set values have the same priority, requests to the domain name will be routed based on weights. | 2 1 2355 example_server.test.com |
| NS | Delegates subdomains to other name servers. | DNS server address<br>You can enter up to 50 values, each on a separate line. | ns1.example.net<br>ns2.example.net |

| Record Set Type | Description | Value | Example |
| --- | --- | --- | --- |
| SOA | Identifies the base information about a domain name. The SOA record set is automatically generated by the DNS service and cannot be added manually. | This type of record set is created by default and cannot be added manually. | This type of record set is created by default and cannot be added manually. |
| PTR | Maps IP addresses to domain names. | Private domain name mapped to the private IP address. You can enter only one domain name. | www.example.com |

## 4.2.2 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 each type 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 on the left, choose **Private Zones**.
   The zone list is displayed.
4. Click  on the upper left and select the desired region and project.
5. Locate the zone and click **Manage Record Set** in the **Operation** column.
6. Click **Add Record Set**.
   The **Add Record Set** dialog box is displayed.
7. Configure the parameters based on **Table 4-3**.

**Table 4-3** Parameters for adding an A record set

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Prefix of the domain name to be resolved.<br>For example, if the domain name is **example.com**, the prefix can be as follows:<br>• **www**: The domain name is www.example.com, which is usually used for a website.<br>• Left blank: The domain name is example.com.<br>To use an at sign (@) as the domain name prefix, just leave this parameter blank.<br>• **abc**: The domain name is abc.example.com, a subdomain of example.com.<br>• **mail**: The domain name is mail.example.com, which is usually used for email servers.<br>• *: 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.<br>A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set. | A – Map domains to IPv4 addresses |
| TTL (s) | Cache duration of the record set on a local DNS server, in seconds.<br>The value ranges from **1** to **2147483647**, and the default value is **300**.<br>If your service address changes frequently, set TTL to a smaller value. | 300 |
| Value | IPv4 addresses mapped to the domain name.<br>You can enter up to 50 values, each on a separate line. | 192.168.12.2<br>192.168.12.3 |
| Tag | (Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 10 tags to a record set.<br>For details about tag key and value requirements, see **Table 4-4**. | example_key1<br>example_value1 |
| Description | (Optional) Supplementary information about the record set.<br>The description can contain no more than 255 characters. | - |

**Table 4-4** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value1 |

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

   The added record set is in the **Normal** state.

### Related Operations

For details about how to configure A record sets, see **Configuring Private Domain Name Resolution for ECSs**.

## 4.2.3 Adding a CNAME Record Set

### Scenarios

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

For more information about each type of record sets, 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 on the left, choose **Private Zones**.

   The zone list is displayed.

4. Click  on the upper left and select the desired region and project.
5. Locate the zone and click **Manage Record Set** in the **Operation** column.
6. Click **Add Record Set**.
   The **Add Record Set** dialog box is displayed.
7. Configure the parameters based on **Table 4-5**.

**Table 4-5** Parameters for adding a CNAME record set

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Prefix of the domain name to be resolved.<br>For example, if the domain name is **example.com**, the prefix can be as follows:<br>• **www**: The domain name is www.example.com, which is usually used for a website.<br>• Left blank: The domain name is example.com.<br>To use an at sign (@) as the domain name prefix, just leave this parameter blank.<br>• **abc**: The domain name is abc.example.com, a subdomain of example.com.<br>• **mail**: The domain name is mail.example.com, which is usually used for email servers.<br>• *: 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<br>A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set. | CNAME – Map one domain to another |
| TTL (s) | Cache duration of the record set on a local DNS server, in seconds.<br>The value ranges from **1** to **2147483647**, and the default value is **300**.<br>If your service address changes frequently, set TTL to a smaller value. | 300 |
| Value | Domain name alias. You can enter only one domain name. | webserver01.example.com |

| Parameter | Description | Example Value |
| --- | --- | --- |
| Tag | (Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 10 tags to a record set.<br>For details about tag key and value requirements, see **Table 4-6**. | example_key1<br>example_value 1 |
| Description | (Optional) Supplementary information about the record set.<br>The description can contain no more than 255 characters. | - |

**Table 4-6** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value 1 |

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

   The added record set is in the **Normal** state.

## 4.2.4 Adding an MX Record Set

### Scenarios

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

For more information about each type 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 on the left, choose **Private Zones**.
   The zone list is displayed.
4. Click  on the upper left and select the desired region and project.
5. Locate the zone and click **Manage Record Set** in the **Operation** column.
6. Click **Add Record Set**.
   The **Add Record Set** dialog box is displayed.
7. Configure the parameters based on **Table 4-7**.

**Table 4-7** Parameters for adding an MX record set

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Prefix of the domain name to be resolved.<br>For example, if the domain name is **example.com**, the prefix can be as follows:<br>• **www**: The domain name is www.example.com, which is usually used for a website.<br>• Left blank: The domain name is example.com.<br>To use an at sign (@) as the domain name prefix, just leave this parameter blank.<br>• **abc**: The domain name is abc.example.com, a subdomain of example.com.<br>• **mail**: The domain name is mail.example.com, which is usually used for email servers.<br>• *: 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<br>A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set. | MX – Map domains to email servers |

| Parameter | Description | Example Value |
| --- | --- | --- |
| TTL (s) | Cache duration of the record set on a local DNS server, in seconds.<br>The value ranges from **1** to **2147483647**, and the default value is **300**.<br>If your service address changes frequently, set TTL to a smaller value. | 300 |
| Value | Email server address<br>You can enter up to 50 values, each on a separate line.<br>The format is **[priority] [mail server host name]**.<br>Configuration rules:<br>• **priority**: priority for an email server to receive emails. A smaller value indicates a higher priority.<br>• **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 up to 10 tags to a record set.<br>For details about tag key and value requirements, see **Table 4-8**. | example_key1<br>example_value1 |
| Description | (Optional) Supplementary information about the record set.<br>The description can contain no more than 255 characters. | - |

**Table 4-8** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value1 |

8. Click **OK**.
9. Switch back to the **Record Sets** tab.
   The added record set is in the **Normal** state.

## 4.2.5 Adding an AAAA Record Set

### Scenarios

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

For more information about each type of record sets, 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 on the left, choose **Private Zones**.
   The zone list is displayed.
4. Click  on the upper left and select the desired region and project.
5. Locate the zone and click **Manage Record Set** in the **Operation** column.
6. Click **Add Record Set**.
   The **Add Record Set** dialog box is displayed.
7. Configure the parameters based on **Table 4-9**.

**Table 4-9** Parameters for adding an AAAA record set

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Prefix of the domain name to be resolved.<br>For example, if the domain name is **example.com**, the prefix can be as follows:<br>• **www**: The domain name is www.example.com, which is usually used for a website.<br>• Left blank: The domain name is example.com.<br>To use an at sign (@) as the domain name prefix, just leave this parameter blank.<br>• **abc**: The domain name is abc.example.com, a subdomain of example.com.<br>• **mail**: The domain name is mail.example.com, which is usually used for email servers.<br>• *: 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.<br>A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set. | AAAA – Map domains to IPv6 addresses |
| TTL (s) | Cache duration of the record set on a local DNS server, in seconds.<br>The value ranges from **1** to **2147483647**, and the default value is **300**.<br>If your service address changes frequently, set TTL to a smaller value. | 300 |
| Value | IPv6 addresses mapped to the domain name.<br>You can enter up to 50 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 up to 10 tags to a record set.<br>For details about tag key and value requirements, see **Table 4-10**. | example_key1<br>example_value1 |

| Parameter | Description | Example Value |
| --- | --- | --- |
| Description | (Optional) Supplementary information about the record set.<br>The description can contain no more than 255 characters. | - |

**Table 4-10** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value1 |

8. Click **OK**.
9. Switch back to the **Record Sets** tab.
   The added record set is in the **Normal** state.

## 4.2.6 Adding a TXT Record Set

### Scenarios

A TXT record set provides description for a domain name.

For more information about each type of record sets, 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 on the left, choose **Private Zones**.
   The zone list is displayed.
4. Click  on the upper left and select the desired region and project.
5. Locate the zone and click **Manage Record Set** in the **Operation** column.

6. Click **Add Record Set**.
   The **Add Record Set** dialog box is displayed.
7. Configure the parameters based on **Table 4-11**.

**Table 4-11** Parameters for adding a TXT record set

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Prefix of the domain name to be resolved.<br>For example, if the domain name is **example.com**, the prefix can be as follows:<br>• **www**: The domain name is www.example.com, which is usually used for a website.<br>• Left blank: The domain name is example.com.<br>To use an at sign (@) as the domain name prefix, just leave this parameter blank.<br>• **abc**: The domain name is abc.example.com, a subdomain of example.com.<br>• **mail**: The domain name is mail.example.com, which is usually used for email servers.<br>• *: 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<br>A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set. | TXT – Specify text records |
| TTL (s) | Cache duration of the record set on a local DNS server, in seconds.<br>The value ranges from **1** to **2147483647**, and the default value is **300**.<br>If your service address changes frequently, set TTL to a smaller value. | 300 |

| Parameter | Description | Example Value |
| --- | --- | --- |
| Value | Text content<br>Configuration rules:<br>• Text record values must be enclosed in double quotation marks.<br>• One or more text record values are supported, each on a separate line.<br>A maximum of 50 text record values can be entered.<br>• A single text record value can contain multiple character strings, each of which is double quoted and separated from others using a space.<br>One character string cannot exceed 255 characters.<br>A value must not exceed 4096 characters.<br>• The value cannot be left blank.<br>• The text cannot contain a backslash (\). | • Single text record:<br>"aaa"<br>• Multiple text records:<br>"bbb"<br>"ccc"<br>• A text record that contains multiple strings:<br>"ddd" "eee" "fff" |
| Tag | (Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 10 tags to a record set.<br>For details about tag key and value requirements, see **Table 4-12**. | example_key1<br>example_value 1 |
| Description | (Optional) Supplementary information about the record set.<br>The description can contain no more than 255 characters. | - |

**Table 4-12** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value 1 |

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

   The added record set is in the **Normal** state.

## 4.2.7 Adding an SRV Record Set

### Scenarios

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

For more information about each type of record sets, 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 on the left, choose **Private Zones**.

   The zone list is displayed.
4. Click  on the upper left and select the desired region and project.
5. Locate the zone and click **Manage Record Set** in the **Operation** column.
6. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
7. Configure the parameters based on **Table 4-13**.

**Table 4-13** 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<br>The format is *_Service name._Protocol*. | _ftp._tcp<br>**_ftp._tcp** indicates that the host provides the FTP service over TCP. |
| Type | Type of the record set<br>A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set. | SRV – Record servers providing specific services |

| Parameter | Description | Example Value |
| --- | --- | --- |
| TTL (s) | Cache duration of the record set on a local DNS server, in seconds.<br>The value ranges from **1** to **2147483647**, and the default value is **300**.<br>If your service address changes frequently, set TTL to a smaller value. | 300 |
| Value | Server address<br>You can enter up to 50 values, each on a separate line.<br>The value format is **[priority] [weight] [port number] [server address]**.<br>Configuration rules:<br>• The priority, weight, and port number range from 0 to 65535.<br>• A smaller value indicates a higher priority.<br>• A larger value indicates a larger weight.<br>• The server address is the domain name of the target server.<br>Ensure that the domain name can be resolved.<br>**NOTE**<br>If the record set values have the same priority, requests to the domain name will be routed based on weights. | 2 1 2355 example_server.test.com |
| Tag | (Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 10 tags to a record set.<br>For details about tag key and value requirements, see **Table 4-14**. | example_key1<br>example_value1 |
| Description | (Optional) Supplementary information about the record set.<br>The description can contain no more than 255 characters. | - |

**Table 4-14** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value1 |

8. Click **OK**.
9. Switch back to the **Record Sets** tab.
   The added record set is in the **Normal** state.

## 4.2.8 Adding a PTR Record Set

### Scenarios

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

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

### Constraints

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

### Procedure

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click  on the upper left and select the desired region and project.
5. Locate the zone and click **Manage Record Set** in the **Operation** column.
6. Click **Add Record Set**.
   The **Add Record Set** dialog box is displayed.
7. Configure the parameters based on **Table 4-15**.

**Table 4-15** Parameters for adding a PTR record set

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Name of the PTR record set | 10.1.168<br>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**.<br>• If the domain name is 192.in-addr.arpa, enter **10.1.168**.<br>• If the domain name is 1.168.192.in-addr.arpa, enter **10**. |
| Type | Type of the record set<br>A message may be displayed indicating that the record set you are trying to add conflicts with an existing record set. | PTR – Map IP addresses to domains |
| TTL (s) | Cache duration of the record set on a local DNS server, in seconds.<br>The value ranges from **1** to **2147483647**, and the default value is **300**.<br>If your service address changes frequently, set TTL to a smaller value. | 300 |
| Value | Private domain name mapped to the private IP address. You can enter only one domain name. | host.example.com. |
| Tag | (Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 10 tags to a record set.<br>For details about tag key and value requirements, see **Table 4-16**. | example_key1<br>example_value1 |
| Description | (Optional) Supplementary information about the record set.<br>The description can contain no more than 255 characters. | - |

**Table 4-16** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value1 |

8. Click **OK**.
9. Switch back to the **Record Sets** tab.
   The added record set is in the **Normal** state.

## Related Operations

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

# 4.3 Managing Record Sets

## Scenarios

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

## Modifying a Record Set

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

NOTE

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

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.
   The zone list is displayed.
4. Click on the upper left and select the desired region and project.
5. In the zone list, locate the zone and click the domain name.
   The **Record Sets** tab is displayed.

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

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

7. Modify the parameters.

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

8. Click **OK**.

## Deleting a Record Set

NOTE

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

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

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

   The DNS console is displayed.

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

   The zone list is displayed.

4. Click  on the upper left and select the desired region and project.
5. In the zone list, locate the zone and click the domain name.

   The **Record Sets** tab is displayed.

6. Locate the record set you want to delete and click **Delete** in the **Operation** column.
7. In the displayed 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 on the left, choose **Private Zones**.

   The zone list is displayed.

4. Click  on the upper left and select the desired region and project.
5. In the zone list, locate the zone and click the domain name.

   The **Record Sets** tab is displayed.

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

# 4.4 Configuring a Wildcard DNS Record Set

## Scenarios

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

NOTE

Exact match has a higher priority than fuzzy match.

## Constraints

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

## Procedure

1. Log in to the management console.
2. In the service list, choose **Network** > **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane on the left, choose **Private Zones**.
   The zone list is displayed.
4. Click  on the upper left 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 4-17**.

**Table 4-17** Parameters for adding a wildcard DNS record set

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Private domain name<br>Enter an asterisk (*) as the leftmost label of the domain name, for example, ***.example.com**.<br>**NOTE**<br>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<br>Wildcard DNS resolution does not support NS and SOA record sets. | A – Map domains to IPv4 addresses |

| Parameter | Description | Example Value |
| --- | --- | --- |
| TTL (s) | Cache duration of the record set on a local DNS server, in seconds.<br>The value ranges from **1** to **2147483647**, and the default value is **300**.<br>If your service address changes frequently, set TTL to a smaller value. | 300 |
| Value | Record set value | Take an A record set for example, **Value** is set to IPv4 addresses mapped to the domain name. Example:<br>192.168.12.2<br>192.168.12.3 |
| Tag | (Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 10 tags to a record set.<br>For details about tag key and value requirements, see **Table 4-18**. | example_key1<br>example_value1 |
| Description | (Optional) Supplementary information about the record set.<br>The description can contain no more than 255 characters. | This is a wildcard DNS record set. |

**Table 4-18** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value1 |

8. Click **OK**.

9. Switch back to the **Record Sets** tab.
   The wildcard DNS record set in the **Normal** state.

# 5 Permissions Management

## 5.1 Creating a User and Granting DNS Permissions

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

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing DNS resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- 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.

**Figure 5-1** shows the process of granting permissions.

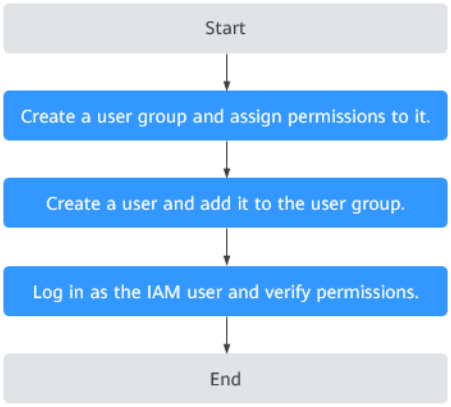
### Prerequisites

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

### Process Flow

**Figure 5-1** Process for granting permissions




1. Create a user group and assign permissions.

   After creating a user group on the IAM console, click **Authorize** in the **Operation** column and assign the read-only permissions to the group.

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

   After creating a user on the IAM console, click **Authorize** in the **Operation** column to add it to the user group created in 1.

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

   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 from **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.<br>• Global-level condition key: The prefix is g:, which applies to all operations, as shown in **Table 5-2**.<br>• 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. Private zones and record sets all have different quota limits. Quotas are put in place to prevent excessive resource usage and ensure service availability.

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

## How Do I View My Quotas?

1. Log in to the management console.
2. In the upper right corner of the page, click  .

   The **Quotas** page is displayed.
3. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

## How Do I Apply for a Higher Quota?

The system does not support online quota adjustment. If you need to adjust a quota, contact the operations administrator.

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

- Account name, 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 on the **My Credentials** page.
- Quota information, which includes service name, quota type, and required quota

# 7 FAQ

## 7.1 DNS Overview

### 7.1.1 Will I Be Billed for the DNS Service?

DNS is a free service.

### 7.1.2 How Many Zones and Record Sets Can I Create?

The default quotas for an account are 50 private zones and 500 record sets.

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

### 7.1.3 Does DNS Support Wildcard Entries?

Yes. DNS allows you to configure wildcard entries.

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

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

### 7.1.4 How Are Zones Queried to Resolve a Domain Name?

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

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

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

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

## 7.1.5 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 have specified. For more information, see RFC 1035.

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

## 7.1.6 Can DNS Point a Domain Name to a Specific Port?

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

# 7.2 Private Zones

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

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

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

**NOTE**

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

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

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

### Creating a Private Zone

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

   The DNS console is displayed.

3. In the navigation pane on the left, choose **Private Zones**.
   The **Private Zones** page is displayed.
4. Click  on the upper left and select the desired region and project.
5. Click **Create Private Zone**.
6. Configure the parameters based on **Table 7-1**.

**Table 7-1** Parameters for creating a private zone

| Parameter | Description | Example Value |
| --- | --- | --- |
| Domain Name | Domain name you use to access the cloud servers or cloud services.<br>Ensure that the domain name suffix is **in-addr.arpa**. | 192.in-addr.arpa |
| VPC | VPC to be associated with the private zone.<br>Select the VPC you want to associate with the private zone. | - |
| Email | (Optional) Email address of the administrator managing the private zone.<br>Recommended email address: **HOSTMASTER@*Domain name***<br>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 private zone.<br>Each tag contains a key and a value. You can add up to 10 tags to a zone.<br>For details about tag key and value requirements, see **Table 7-2**. | example_key1<br>example_value1 |
| Description | (Optional)<br>Supplementary information about the zone.<br>The description can contain no more than 255 characters. | This is a private zone. |

**Table 7-2** Tag key and value requirements

| Parameter | Requirements | Example Value |
| --- | --- | --- |
| Key | • Cannot be left blank.<br>• Must be unique for each resource.<br>• Can contain no more than 36 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_key1 |
| Value | • Cannot be left blank.<br>• Can contain no more than 43 characters.<br>• Cannot start or end with a space nor contain special characters =*<>\,\|/ | example_value1 |

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

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

   NOTE

   You can click the domain name to view SOA and NS record sets automatically added to the zone.

   - The SOA record set includes administrative information about your zone, as defined by the Domain Name System (DNS).
   - The NS record set defines the authoritative DNS servers for the domain name.

## Adding a PTR Record Set

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

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

   The **Add Record Set** dialog box is displayed.
3. Configure the parameters based on **Table 7-3**.

**Table 7-3** Parameters for adding a PTR record set

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Part of the private IP address in reverse order. | 10.1.168<br>For example, if the IP address is 192.168.1.10, the domain name in the PTR record must be 10.1.168.192.in-addr.arpa.<br>• If the domain name is 192.in-addr.arpa, enter **10.1.168**.<br>• If the domain name is 1.168.192.in-addr.arpa, enter **10**. |
| Type | Type of the record set. | PTR – Map IP addresses to domains |
| TTL (s) | Cache duration of the record set, in seconds. | Default value: 300 |
| Value | Domain name mapped to the IP address.<br>You can enter only one name. | mail.example.com |
| Tag | (Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 10 tags to a record set.<br>For details about tag key and value requirements, see **Table 7-2**. | example_key1<br>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** tab.

   The added record set is in the **Normal** state.

# A Change History

| Released On | Description |
| --- | --- |
| 2024-11-30 | This issue is the first official release. |