Domain Name Service

User Guide

Issue 01

Date 2025-08-25

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 Using IAM to Grant Access to DNS

1.1 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 Huawei Cloud 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.

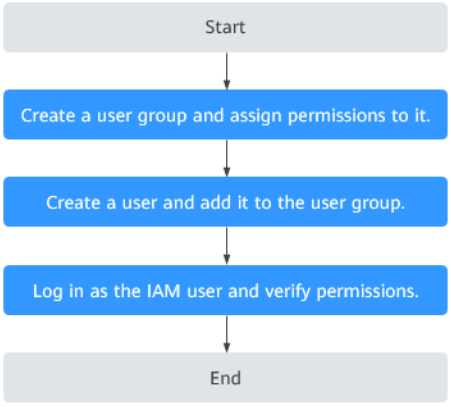
Figure 1-1 shows the process of granting permissions.

Prerequisites

Learn about the permissions (**Permissions Management**) supported by DNS and choose policies or roles based on your requirements. For the permissions of other services, see **System Permissions**.

Process Flow

Figure 1-1 Process for granting permissions



1. .

   After creating a user group on the IAM console, attach the **DNS ReadOnlyAccess** policy to the group, which grants users read-only permissions to DNS resources.
2. The user group is the one you have created in step 1.
3. .

   Verify that the user only has read permissions for DNS.

   - Choose **Service List** > **Domain Name Service**. On the DNS console, choose **Overview** > **Public Zones**. On the displayed page, click **Create Public Zone**. If the public 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.

1.2 Creating Custom Policies

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

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

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

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

For details, see **Creating a Custom Policy**. Some examples of common custom DNS policies are provided.

Example Custom Policies

- Example 1: Authorize users to create zones, add record sets, and view the zones and record sets.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "dns:zone:create",
            "dns:recordset:create",
            "dns:zone:list"
      "dns:recordset:list"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "vpc:*:get*",
            "vpc:*:list*"
         ]
      }
   ]
}
```

- Example 2: Disallow users to delete DNS resources.

  A deny policy must be used together with other policies. If the permissions granted to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **DNS FullAccess** policy to a user but also forbid the user from deleting DNS resources. Create a custom policy to disallow resource deletion and assign both policies to the group the user belongs to. Then the user can perform all operations on DNS except deleting resources. The following is an example deny policy:

```
{
    "Version": "1.1",
    "Statement": [
        {
       "Effect": "Deny",
            "Action": [
                "dns:*:delete*"
            ]
        }
    ]
}
```

- Example 3: Create a custom policy containing multiple actions.

  A custom policy can contain actions of multiple services that are all of the global or project-level type. The following is an example policy containing multiple actions:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "dns:zone:update",
            "dns:zone:list"
         ]
      },
      {
         "Effect": "Allow",
```



```
            "Action": [
                "vpc:subnets:create",
                "vpc:vips:update"
            ]
        }
    ]
}
```


2 Public Domain Name Resolution

2.1 Overview

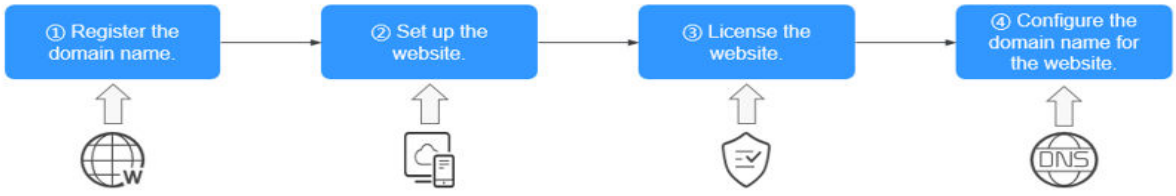
What Is Public DNS Resolution?

Public DNS resolution translates domain names (for example, www.example.com) and their subdomains into IP addresses like 1.2.3.4 for routing traffic over the Internet. Public DNS resolution is implemented by public DNS servers, including authoritative and non-authoritative DNS servers.

Authoritative DNS services are typically provided by either domain name registrars or cloud service providers. Authoritative DNS servers store various DNS records, including A, CNAME, and MX records, and provide accurate responses to DNS queries. DNS provides highly available and scalable authoritative DNS resolution services and domain name management services.

If you host domain names on the Huawei Cloud DNS service, authoritative DNS servers will be provided for public domain name resolution for your website and email server. Visitors can access your website, mailbox, or web application by entering your domain name in the address box of their browser.

Figure 2-1 Accessing a website using a domain name



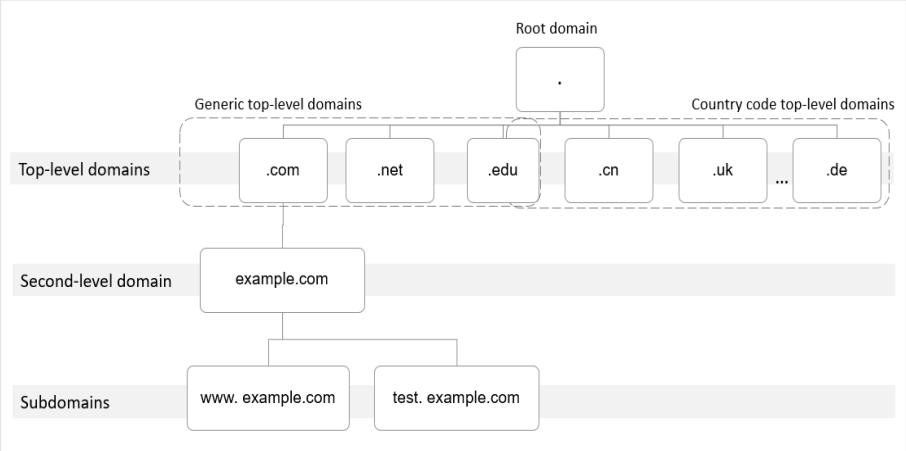
Public Zones

A domain name is registered and purchased through a domain name registrar, for example, Huawei Cloud. DNS service providers like Huawei Cloud Domain Name Service (DNS) are responsible for resolving domain names. You can use DNS to create a public zone for your domain name, which can work for access to portal websites, enterprise emails, and web applications.

Unlike private zones, public zones are designed for external users and prioritize higher security and robust management to handle internet-facing traffic. Private zones are used for internal network services and emphasize limited access scope.

The domain name resolution involves a hierarchical structure and often uses recursive queries.

The following uses example.com as an example to describe the structure and levels of a domain.



- **Root domain**

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

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

  Root domain names are resolved by root name servers that hold the addresses of top-level domain servers.

- **Top-level domain**

  Below the root domain are top-level domains, which are categorized into two types:

  – Generic top-level domain (gTLD), such as .com, .net, .org, and .top

  – Country code top-level domain (ccTLD), such as .cn, .uk, and .de

  Top-level domains are resolved by top-level domain servers that hold the addresses of second-level DNS servers. For example, the top-level domain server of .com saves the addresses of all DNS servers of second-level domains that end with .com.

- **Second-level domain**

  Second-level domains (such as example.com) are subdomains of top-level domains and are resolved by second-level DNS servers, which provide authoritative domain name resolution services.

  For example, if you purchase example.com from a domain name registrar and set a DNS server for the domain name, the DNS server will provide authoritative resolution for example.com, and its address will be recorded by all top-level domain servers.

If you host domain names on the Huawei Cloud DNS service, authoritative DNS servers will provide authoritative resolution services for your domain names.

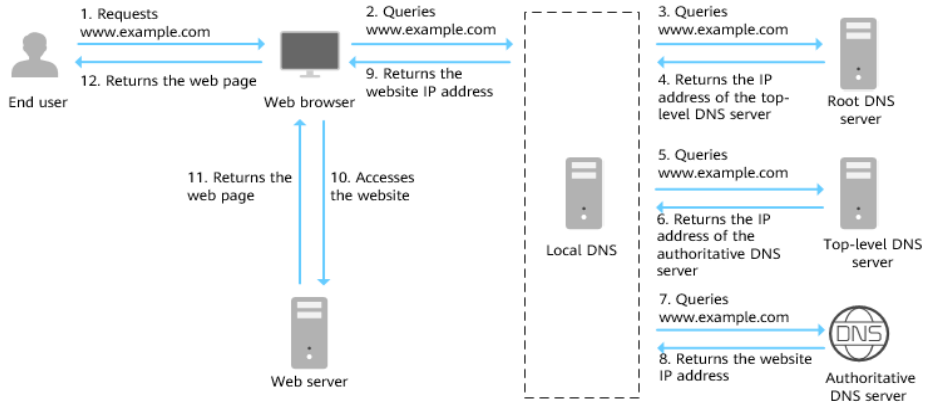
- **Subdomain**

  Second-level domains can be further divided into subdomains (such as www.example.com) to indicate specific servers or services.

Resolution Process

The figure below shows the process for accessing a website using the domain name www.example.com.

Figure 2-2 Domain name resolution



1. An end user enters **www.example.com** in the address box of a browser.
2. The query for www.example.com is routed to the local DNS server.

   Local DNS servers are usually provided by the Internet service provider to cache domain name information and perform recursive lookup.
3. If the local DNS server does not find any records in the cache, it routes the request for www.example.com to the root name server.
4. The root name server returns the address of the top-level domain server of .com to the local DNS server.
5. The local DNS server sends the request to the top-level domain server of .com.
6. The top-level domain server of .com returns the address of the authoritative DNS server which provides authoritative records for example.com.
7. The local DNS server sends the request to the authoritative DNS server of example.com.

   If you have hosted www.example.com on the DNS service and configured **Huawei Cloud DNS name servers**, these name servers will provide authoritative DNS for the domain name.
8. The authoritative DNS server returns the IP address mapped to www.example.com to the local DNS server.
9. The local DNS server returns the IP address to the web browser.
10. The web browser accesses the web server with the IP address.

11. The web server returns the web page to the browser.
12. The end user views the web page using the browser.

2.2 Public Zones

2.2.1 Creating a Public Zone

Scenarios

To use Huawei Cloud DNS for public domain name resolution, create a public zone for your domain name on the DNS console.

This section describes how to create a public zone for your domain name on the DNS console.

Prerequisites

You have registered a domain name.

Procedure

1. Go to the **Public Zones** page.
2. In the upper right corner of the page, click **Create Public Zone**.

   Configure the parameters based on **Table 2-1**.

Table 2-1 Parameters for creating a public zone

Parameter	Description	Example
Domain Name	Domain name purchased from a domain name registrar. For details about the domain name format, see **Domain Name Format and DNS Hierarchy**.	example.com
Email	This parameter is optional. Email address of the administrator managing the public domain name. It is recommended that you set the email address to **HOSTMASTER@***Domain name*. For more information about the email address, see **Why Was the Email Address Format Changed in the SOA Record?**	HOSTMASTER@example.com

Parameter	Description	Example
Enterprise Project	Enterprise project associated with the public zone. You can manage public zones by enterprise project. This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**. When setting this parameter, note the following: • If you do not manage zones by enterprise project, select the **default** enterprise project. • If you manage zones by enterprise project, select an existing enterprise project. Before you configure this parameter, **create an enterprise project**.	default
Tag	This parameter is optional. Identifier of the zone. Each tag contains a key and a value. You can add up to 20 tags to a zone. For details about tag key and value requirements, see **Table 2-2**.	example_key1 example_value1
Description	This parameter is optional. Supplementary information about the zone. The description can contain a maximum of 255 characters.	This is a zone example.

Table 2-2 Tag key and value requirements

Parameter	Requirements	Example
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@	example_key1
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_value1

3. Click **OK**.

   You can view the created zone in the zone list.

   If "This public zone has been created by another account. You need to reclaim it first." is displayed when you create a public zone, you need to **reclaim the public zone**.

   NOTE

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

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

Helpful Links

- To ensure that the domain name can be resolved, Huawei Cloud DNS servers must be used. If not, see **Changing DNS Servers for a Public Domain Name**.
- You can modify, delete, and view details about the public zone. For details, see **Managing Public Zones**.
- You can add record sets for the public zone. For details, see **Adding Record Sets for a Public Zone**.

2.2.2 Creating a Subdomain

Scenarios

A subdomain and its primary domain name are indeed part of the same registered domain. A subdomain is essentially an extension of the primary domain name,

created by adding a prefix (one or more parts) before the primary domain name. You can use subdomains to categorize and separate different types of services, languages, and brands on your website, while also allowing for flexibility in DNS management.

Take example.com as an example. You add the following subdomains for it:

- Subdomains to provide clear navigation paths for different sections of the website, such as www.example.com (main site), blog.example.com (blog), and shop.example.com (online store).
- Subdomains to indicate distinct language-specific sections of the website, such as en.example.com (English) and zh.example.com (Chinese).
- Subdomains for distinct branding and tailored content for each product, for example, productA.example.com and productB.example.com.

Prerequisites

You have registered a domain name.

Procedure

1. Go to the **Public Zones** page.
2. In the upper right corner of the page, click **Create Public Zone**.

   Configure the parameters based on **Table 2-3**.

Table 2-3 Parameters for creating a subdomain

Parameter	Description	Example
Domain Name	Subdomain of the domain name purchased from a domain name registrar. For details about the domain name format, see **Domain Name Format and DNS Hierarchy**.	www.example.com
Email	Optional. Email address of the administrator managing the public domain name. It is recommended that you set the email address to **HOSTMASTER@***Domain name*. For more information about the email address, see **Why Was the Email Address Format Changed in the SOA Record?**	HOSTMASTER@example.com

Parameter	Description	Example
Enterprise Project	Enterprise project associated with the public zone. You can manage public zones by enterprise project. This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**. When setting this parameter, note the following: • If you do not manage zones by enterprise project, select the **default** enterprise project. • If you manage zones by enterprise project, select an existing enterprise project. Before you configure this parameter, **create an enterprise project**.	**default**
Tag	Optional. Identifier of the zone. Each tag contains a key and a value. You can add up to 20 tags to a zone. For details about tag key and value requirements, see **Table 2-4**.	example_key1 example_value1
Description	Optional. Supplementary information about the zone. The description can contain a maximum of 255 characters.	Subdomain of example.com

Table 2-4 Tag key and value requirements

Parameter	Requirements	Example
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@	example_key1
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_value1

3. Click **OK**.

   You can view the created subdomain in the zone list.

   If "This public zone conflicts with a public zone created by another account." is displayed when you create a subdomain, log in to the account of the primary domain name and add a TXT record set for the primary domain name.

   NOTE

   You can click the domain name to view SOA and NS record sets automatically added to the zone. The NS record set defines the authoritative DNS servers for the domain name. The SOA record set identifies the base DNS information about the domain name.

Helpful Links

- You can modify, delete, and view details about the subdomain. For details, see **Managing Public Zones**.
- You can add record sets for a zone. For details, see **Adding Record Sets for a Public Zone**.

2.2.3 Batch Adding Domain Names

Scenarios

If you want to host domain names registered with other DNS service providers on the DNS console, you can add these domain names in batches.

Generally, if your domain name is registered with Huawei Cloud, a public zone will be created automatically, and you can view the domain name on the DNS console.

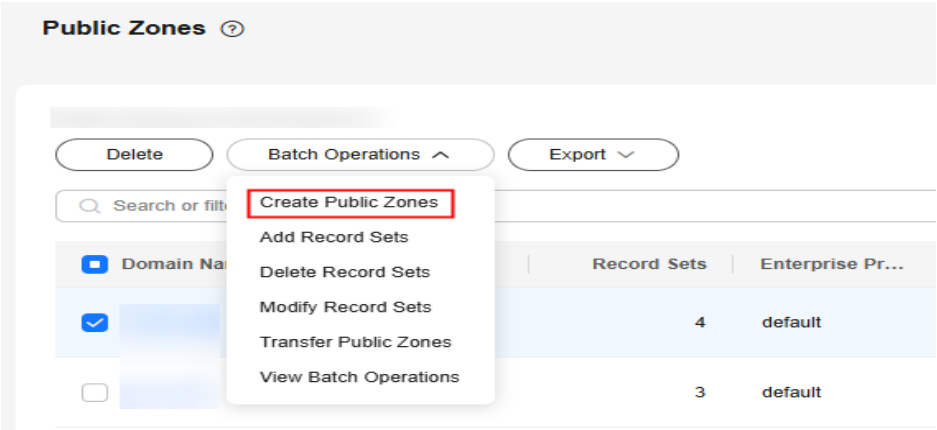
Constraints

- You can enter up to 10,000 domain names at a time.
- Only domain names that are not registered with Huawei Cloud can be added.
- If a public zone has been created for the domain name by another Huawei Cloud account, you can reclaim the public zone by referring to **Reclaiming a Public Zone**.

Procedure

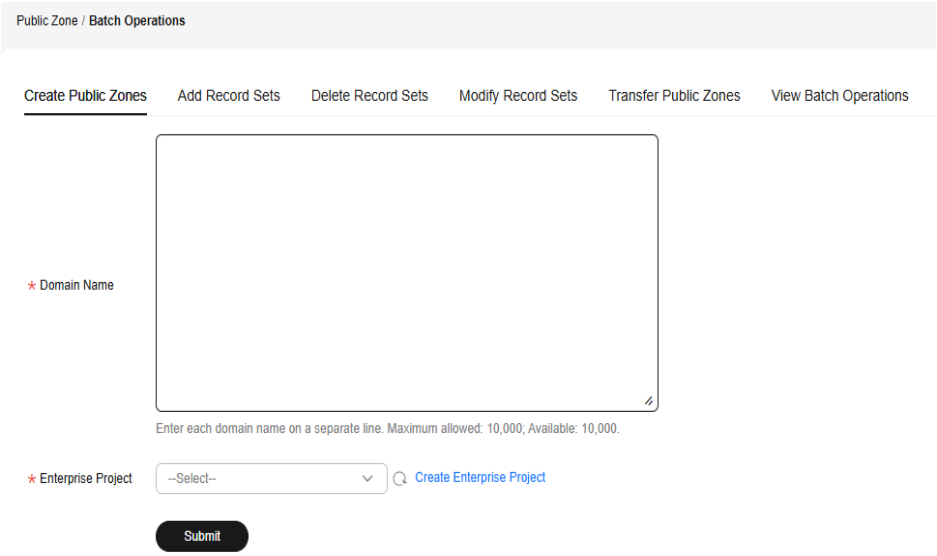
1. Go to the **Public Zones** page.
2. In the **Batch Operations** area above the public zone list, select **Add Domain Names** from the drop-down list.

   Figure 2-3 Add Domain Names



3. On the **Add Domain Names** tab, enter the domain names you want to add and select an enterprise project.

   Figure 2-4 Batching add domain names



4. Click **Submit**.

   After domain names are added, you can view the operation name, result, time, and status on the **View Batch Operations** tab. You can also download failed operations.

2.2.4 Changing DNS Servers for a Public Domain Name

Scenarios

The DNS servers of a domain name indicate the DNS service provider of that domain name.

If you want to configure record sets for a domain name hosted on Huawei Cloud DNS, its DNS servers must be provided by Huawei Cloud DNS. If they are not, the record sets will not be active after you add them. To make such record sets take effect, you need to change the DNS servers to those provided by Huawei Cloud DNS in your domain name registrar's system.

The following are operations for you to change the DNS servers of a domain name.

Changing DNS Servers for a Domain Registered with Huawei Cloud

For domain names registered with Huawei Cloud, you can log in to the Domains console to check their DNS settings.

1. In the domain name list, click the domain name to go to its details page.
2. View and change the DNS servers of the domain name.

   If your domain name is hosted on Huawei Cloud DNS, change the DNS servers to those provided by Huawei Cloud DNS.

   - ns1.huaweicloud-dns.eu
   - ns2.huaweicloud-dns.eu

Changing the DNS Servers for Domain Names Not Registered with Huawei Cloud

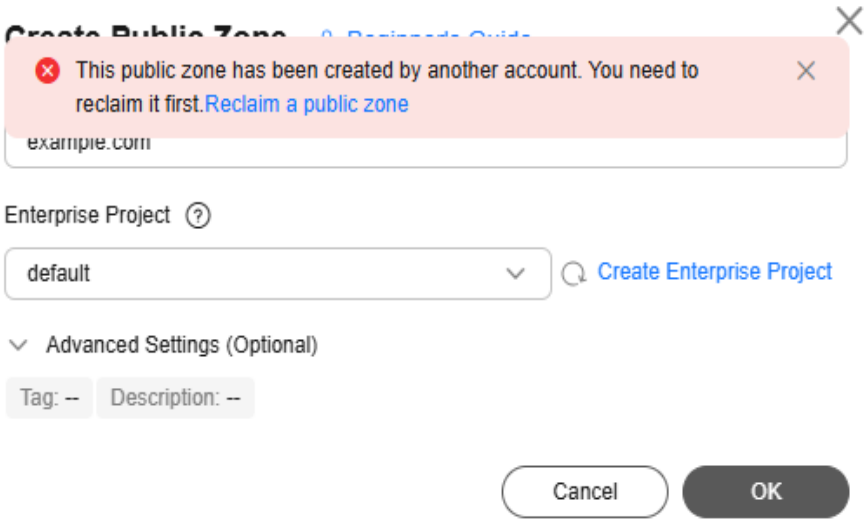
If a domain name is registered with another domain name registrar, go to the system of that registrar and change the DNS servers to those provided by Huawei Cloud DNS.

For details, see the operation guide on the official website of the domain name registrar.

2.2.5 Reclaiming a Public Zone

Scenarios

Assume that you are the owner of a domain name and you are **creating a public zone** for your domain name on the DNS console. If "This public zone has been created by another account. You need to reclaim the public zone first." is displayed when you are creating a public zone, as shown in the following figure, you can reclaim the public zone.



Feature Description

When you reclaim a public zone for a domain name, the DNS console will first generate a TXT record. You need to add this TXT record on your current DNS service provider's platform and then verify the TXT record on the DNS console. The DNS console will request the TXT record over the Internet. If the TXT record value is returned, you are the domain name owner and your public zone will be reclaimed automatically.

CAUTION

- If a public zone is reclaimed, all record sets added to it before will be deleted.
- If DNS resolution is abnormal due to incorrect public zone reclaim operations, you are liable for the risks and consequences.

Domain Name Owner

A domain name is owned by the person or organization who registered it through a domain registrar Details about a domain name owner are as follows:

- **Ownership and control**: Domain name owners have the right to use domain names as they see fit, for example, directing them to specific servers and creating subdomains.
- **Registration and maintenance**: Domain name owners must register their domain names with a registrar and pay annual renewal fees to maintain ownership and prevent expiration.
- **Information management**: Domain name owners are generally required to provide personal information, including their name, address, and email address, during the registration process. This information is stored in a publicly accessible database called the WHOIS database. However, privacy protection services can be used to hide their personal details.

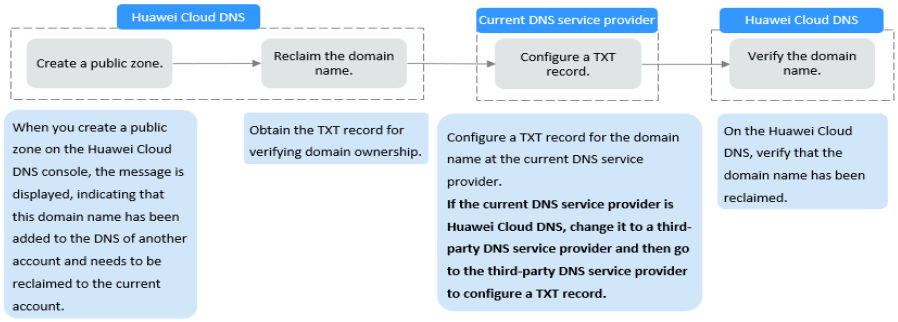
- **Management permissions**: Domain name owners can manage DNS settings, control website resolution, implementing security measures like DKIM and SPF records, and transfer domain names to other registrars.
- **Renewal and transfer**: Domain name owners should renew their domain registrations before the expiration date. Domain names can be transferred through registrars or traded in the secondary market.

DNS Service Provider

A DNS service provider manages the Domain Name System (DNS), which translates domain names into server IP addresses. A DNS service provider provides the following functions:

- **Domain name resolution**: translates domain names into IP addresses so that users can access target websites by entering a domain name.
- **DNS record management**: allows users to set and manage various DNS records, like A, CNAME, and MX records.
- **High availability and stability**: leverages multi-node distribution to ensure the DNS resolution stability and efficiency.
- **Value-added services**: provides functions such as load balancing, CDN integration, anti-DDoS, and intelligent resolution to improve website performance and security.

Process Flow



Procedure

Step 1 Obtain the TXT record.

1. Go to the **Public Zones** page.
2. In the upper right corner of the page, click **Create Public Zone**.
3. Configure the parameters and click **OK**.
4. Click **Reclaim a public zone** in the displayed message.
5. In the **Reclaim Public Zone** dialog, take a note of the TXT record set.

Step 2 Add the TXT record for verification.

The following operations are performed on Alibaba Cloud which is the example DNS service provider. The operations are for reference only. For details, see "Add DNS Records" in the Alibaba Cloud documentation.

1. Log in to the Alibaba Cloud console.
2. In the service list in the upper left corner of the console, choose **Domain Name and Websites** to go to its DNS console.
3. In the navigation pane, choose **Public DNS Resolution** > **Authoritative DNS Resolution**.
4. In the domain name list, click the target domain name in the **Domain Name** column.

   If the target domain name does not exist in the list, click **Add Domain Name**.
5. Add a TXT record for the domain name.
   - Record type: TXT
   - Record name: Enter the record named obtained in **Step 1.5**.
   - Record value: Enter the record value obtained in **Step 1.5**.
6. Confirm the configuration and submit your request.

   If the status of the record becomes **Normal**, the TXT record is added.

Step 3 Verify the TXT record.

Go back to the dialog box shown in **Step 1.5** and click **Verify**.

The DNS console will verify the TXT record. If the verification is successful, a public zone will be created for your domain name.

----End

2.2.6 Managing Public Zones

Scenarios

You can modify, export, enable, disable or delete public zones, or view their details.

Modifying a Public Zone

You can change the domain name administrator's email address and description of the public zone.

NOTE

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

1. Go to the **Public Zones** page.
2. Select the public zone you want to modify, and choose **More** > **Modify** in the **Operation** column.

   The **Modify Public Zone** dialog box is displayed.
3. Modify the public zone.
4. Click **OK**.

Deleting a Public Zone

You can delete a public zone when you no longer need it.

WARNING

After a public zone is deleted, the domain name and its subdomains cannot be resolved by the DNS service. Before you delete a public zone, back up all its record sets.

1. Go to the **Public Zones** page.
2. Locate the public zone you want to delete and click **Delete** in the **Operation** column.
3. In the displayed dialog box, confirm the public zone to be deleted.

   Enter **DELETE** and click **OK**.

Disabling or Enabling a Public Zone

You can disable a public zone to make all its record sets inactive. When you want to restore the resolution of the domain name, enable the public zone.

1. Go to the **Public Zones** page.
2. Select the public zone you want to disable or enable and click **Disable** or **Enable** in the **Operation** column.

   The **Disable Public Zone** or **Enable Public Zone** dialog box is displayed.
3. Click **OK**.

Viewing Details About a Public Zone

On the **Public Zones** page, you can view details about public zones, including the domain name, status, DNS server address, number of record sets, enterprise project, tag, TTL, creation time, last modification time, and description.

NOTE

The latest modification time of a domain name is updated only after the record set is updated. This may cause inconsistency between the latest modification time of the record set and domain name.

1. Go to the **Overview** page.
2. On the **Overview** page, click **Public Zones** under **My Resources**.

2.3 DNS Rules

2.3.1 Record Set Types and Configuration Rules

Record Set Types and Configuration Rules

Record set types for public zones include A, CNAME, MX, AAAA, TXT, SRV, NS, SOA, and CAA. For details, see **Table 2-5**.

Table 2-5 Record set types and configuration rules

Record Set Type	Description	Rule	Example
A	Maps domains to IPv4 addresses. It is usually used to map domain names used by websites to IPv4 addresses.	Enter IPv4 addresses mapped to the domain name. You can enter up to 50 different IP addresses, each on a separate line.	1.1.*xx.xx* 1.2.*xx.xx*
CNAME	Maps one domain name to another domain name or multiple domain names to one domain name.	Enter the mapped domain name. You can enter only one domain name.	www.example.com

Record Set Type	Description	Rule	Example
MX	Maps domain names to email servers.	Enter email server addresses. You can enter up to 50 different IP addresses, 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	Maps domain names to IPv6 addresses.	Enter IPv6 addresses mapped to the domain name. You can enter up to 50 different IP addresses, each on a separate line.	ff03:0db8:85a3:0:0:8a2e:0370:7334

Record Set Type	Description	Rule	Example
TXT	Creates text records for domain names. It is usually used in the following scenarios: • To record DKIM public keys to prevent email fraud. • To record the identity of domain name owners to facilitate domain name retrieval.	Enter text content as required. 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 4,096 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" • Text record in SPF format: "v=spf1 a mx -all" This value indicates that only IP addresses in the A and MX record sets are allowed to send emails using this domain name.

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

Record Set Type	Description	Rule	Example
NS	Delegates subdomains to other name servers. After a public zone is created, an NS record set is automatically created for this zone and cannot be deleted. You can add NS record sets only in the following scenarios: • The **Name** parameter is not left blank. This means that you can add NS record sets for subdomains of a domain name. • The value of the **Line** parameter is not set to **Default**. This means that you can add NS record sets for the domain name with other resolution lines.	Enter the DNS server address. You can enter up to 50 different IP addresses, each on a separate line.	ns1.example.com ns2.example.com
SOA	Identifies the base information about a domain name. The SOA record set is automatically generated by the DNS service and cannot be added manually.	This type of record set is created by default and cannot be added manually.	This type of record set is created by default and cannot be added manually.

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

Record Set Type	Description	Rule	Example
		once a CA receives invalid certificate requests. • **value**: authorized CA or email address/URL required for notification once the CA receives invalid certificate requests. The value depends on the value of **tag** and must be enclosed in quotation marks (""). The value can contain a maximum of 255 characters. Only letters, digits, spaces, and the following special characters are allowed: -#*? &_~=:;.@+^/!%	

Wildcard Resolution Rules

DNS allows you to add a record set with the record set name set to an asterisk (*), for example, *.example.com. This can map all subdomains to the same value.

If you have added a wildcard record set for a domain name and added multiple record sets of the same type but different line for a specific subdomain, the DNS resolution complies with the following rules:

- **Priority**: Line match has a higher priority than domain name match.
- **Priority of queries in the same line**: If the line type is the same, exact match has a higher priority than fuzzy match.
- **Priority for interaction between intelligent resolution and default lines**: Wildcard domain name query matches the intelligent line, and exact domain

name query matches the default line. If both of them are matched, the exact domain name query result prevails.

Take example.com as an example.

1. Configure wildcard records and a record for the subdomain starting with www.

   The following table lists the parameter settings.

Subdomain	Line	Record Set Type	Value
www.example.com	Default	A	4.4.xx.xx
*.example.com	Default line for China Telecom	A	1.1.*xx.xx*
*.example.com	Default line for China Unicom	A	2.2.xx.xx
*.example.com	Default line for China Mobile	A	3.3.xx.xx

   When a visitor is a China Telecom, China Unicom, or China Mobile user, **4.4.xx.xx** is returned.

   Rule: If both wildcard and exact domain name queries are matched, the exact domain name query result prevails.

2. Configure intelligent resolution for the subdomain www.example.com.

Subdomain	Line	Record Set Type	Value
www.example.com	**Default**	**A**	**4.4.xx.xx**
*.example.com	Default line for China Telecom	A	1.1.*xx.xx*
www.example.com	**Default line for China Telecom**	**A**	**1.1.xx.xx**
*.example.com	Default line for China Unicom	A	2.2.xx.xx
www.example.com	**Default line for China Unicom**	**A**	**2.2.xx.xx**
*.example.com	Default line for China Mobile	A	3.3.xx.xx
www.example.com	**Default line for China Mobile**	**A**	**3.3.xx.xx**

   When visitors are China Telecom, China Unicom, or China Mobile users and they are accessing www.example.com, **1.1.xx.xx** is returned for the China

Telecom user, **2.2.xx.xx** is returned for the China Unicom user, and **3.3.xx.xx** is returned for the China Mobile user.

Rule: Line match has a higher priority than domain name match. If the line type is the same, exact match has a higher priority than fuzzy match.

TTL Setting Rules

TTL (time to live) specifies how long records are cached on a local DNS server. The TTL value, typically measured in seconds, dictates the validity period of the cached record. Common TTL values for DNS records include 300 seconds (5 minutes), 3,600 seconds (1 hour), and 86,400 seconds (24 hours). The default TTL value for Huawei Cloud DNS is 300 seconds.

When receiving requests for a domain name, the local DNS server asks the authoritative DNS server for the required DNS record, and then caches the record for a period of time, as defined by the TTL value specified in the record.

- During this TTL period, if the local DNS server receives requests for this domain name again, it will not request the record from the authoritative DNS server, but directly returns the cached record.
- When the TTL expires, the local DNS server clears the cached record. If the local DNS server receives new DNS queries for the domain name, it forwards the new DNS queries to the authoritative DNS server to obtain the latest resolution result and caches the result.

Table 2-6 Application scenarios of TTL

TTL Setting	Scenarios	Description
Increase the TTL value.	Reducing network traffic	A larger TTL value allows DNS records to be cached on the client or server for a longer period, leading to fewer queries to the authoritative DNS servers and reduced network load.
	Faster response	In IP packets, a larger TTL value allows packets to survive longer on the network. This helps reduce the number of retransmission requests and prevent network congestion.
	Stable network	In a stable network with low packet loss, a large TTL value can improve data transmission efficiency by avoiding the need for retransmissions.

TTL Setting	Scenarios	Description
Decrease the TTL value.	Quick update	• For frequently updated content such as that from news websites or social media, a small TTL ensures that users can obtain the latest information in a timely manner, reducing the delay caused by caching. • A small TTL can quickly clear the old cache and ensure faster update of DNS records. This ensures that the clients can use the latest records sooner.
	Testing and diagnosis	In network testing, a small TTL value is beneficial for quickly identifying and troubleshooting network issues. By setting a low TTL, packets are designed to expire quickly, which makes them easy to trace and analyze.
	Dynamic network environment	A small TTL value can minimize the impact of outdated routing data on a network where routes are frequently changing. This improves network adaptability and response speed.
	Reducing network congestion	A small TTL value can help prevent network congestion, particularly in bandwidth-constrained environments.

To set the TTL value, you need to consider both the stability and update requirements of records. For stable records, set a large TTL value, while for frequently changed records, set a small TTL value. Pay attention to the following points:

- **A balance between load and response**: When adjusting the TTL value, you need to balance the network load and response speed. This aims to prevent delays in updates out of a high TTL value or load increase out of a low TTL value.
- **Network environment evaluation**: You need to set an appropriate TTL value after considering both the network stability and packet loss rate.
- **Monitoring and testing**: After adjusting the TTL value, you need to monitor and test its impact to ensure the desired outcome and make further adjustments if needed.
- **Change management**: Before changing a DNS record, such as changing the server IP address, you are advised to reduce the TTL value so that DNS caches expire faster, allowing for quicker adoption of the new record. Once the change is fully propagated, the TTL can be restored to its original value.

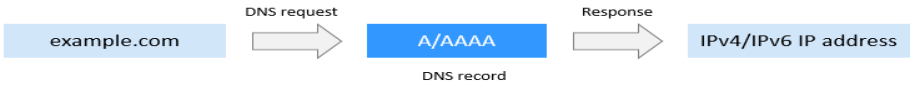
Record Set Application Example

Record sets are used in following scenarios:

- Routing Internet traffic to a website

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

  Figure 2-5 Accessing a website over the Internet using domain name



- Private domain name resolution

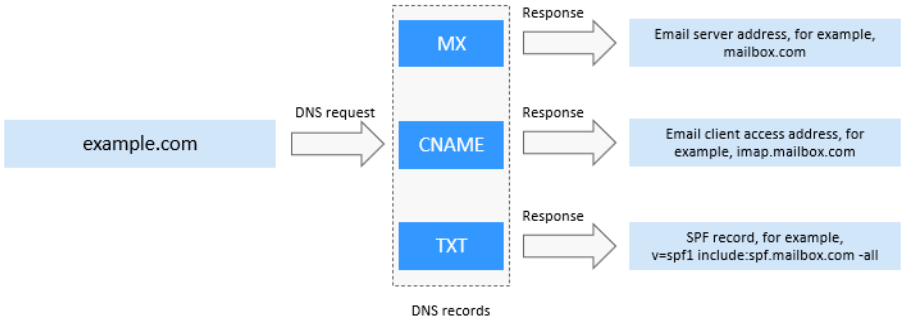
  On a private network, A and AAAA record sets translate private domain names into private IP addresses.

  Figure 2-6 Private domain name resolution

- Email domain name resolution

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

  Figure 2-7 Email domain name resolution



- Reverse resolution on a private network

  PTR records translate private IP addresses into private domain names.

  Figure 2-8 Reverse resolution on a private network

2.3.2 Rules for Handling Record Set Conflicts

Causes for Record Set Conflicts

Some record sets of the same name and line but different types cannot coexist. Otherwise, the resolution fails.

The possible causes are as follows:

- **CNAME record set restrictions**: A CNAME record set cannot coexist with record sets of other types. For example, if a subdomain already has a CNAME record set configured, it cannot have other types of record sets, such as A, MX, and TXT. Otherwise, resolution may fail.
- **Resolution sequence and priority**: The DNS server resolves a domain name based on the record set type and priority. Improper configuration may cause resolution failure or conflict.
- **Multiple resolution paths**: If a domain name has multiple record sets of different types, the DNS server resolves the domain name through different paths. This results in inconsistent or conflicting resolution results.

According to the DNS standard RFC protocol, the CNAME record set has the highest priority. If CNAME and other types (such as MX) of record sets coexist, the CNAME record set hijacks MX record set in specific scenarios. As a result, the mailbox cannot send or receive emails.

For example, if the local DNS has requested and cached the CNAME record set, when the client requests the MX record set (using the mailbox to send emails), the local DNS preferentially returns the cached CNAME record set instead of requesting the MX record set from the Internet. In this case, the MX record set of the email server cannot be obtained. As a result, the mailbox fails to send emails.

Record Set Conflict Rules

If message "This record set is in conflict with an existing one" is displayed, the record set you are trying to add conflicts with or is the same as an existing record set.

Table 2-7 lists the rules.

Table 2-7 Conflicts between public zone record sets

Record Set Type	NS	CNAME	A	AAAA	MX	TXT	PTR	SRV	CAA
NS	**No limit**[a]	**Conflict**	No limit	No limit	No limit	No limit	No limit	No limit	No limit
CNAME	**Conflict**[b]	No limit	**Conflict**	**Conflict**	**Conflict**	**Conflict**	**Conflict**	**Conflict**	**Conflict**
A	No limit	**Conflict**	No limit	No limit	No limit	No limit	No limit	No limit	No limit
AAAA	No limit	**Conflict**	No limit	No limit	No limit	No limit	No limit	No limit	No limit
MX	No limit	**Conflict**	No limit	No limit	No limit	No limit	No limit	No limit	No limit
TXT	No limit	**Conflict**	No limit	No limit	No limit	No limit	No limit	No limit	No limit

PTR	No limit	**Conflict**	No limit	No limit	No limit	No limit	No limit	No limit	No limit
SRV	No limit	**Conflict**	No limit	No limit	No limit	No limit	No limit	No limit	No limit
CAA	No limit	**Conflict**	No limit	No limit	No limit	No limit	No limit	No limit	No limit

- **Conflict**: The two types of record sets cannot coexist for the same name and line.
- **No limit**: The two types of record sets can coexist.
- a: NS record sets cannot be added for second-level domain names. There is no such restriction on subdomains.
- b: For second-level domain names, CNAME and NS record sets can coexist. For subdomains, CNAME record sets conflict with NS record sets.

Record Set Conflict Troubleshooting

Conflict Between CNAME and MX Record Sets

If your enterprise purchases a domain name for end users to access the website of your enterprise and for employees to access the office mailbox of your enterprise. Appropriate record set configuration is necessary.

For access acceleration or secure purposes, cloud services such as CDN, WAF, and OBS are configured for the website. In this case, A record sets cannot be configured to map the domain name to the IP address of the website. Instead, CNAME record sets are required to map the domain name to the domain name of the cloud service such as CDN, WAF, or OBS. The standard DNS protocol does not allow the same domain name to have both CNAME record sets and other types of record sets such as MX record sets at the same time. If a domain name is used for accessing the website and for accessing the enterprise office mailbox as well, the mailbox may be unavailable when there is a conflict between CNAME record sets and MX record sets.

- (Recommended) Universal Solution

  Domain name example.com is used as an example here. Configuration details are as follows.

  - **Accessing a website**

    i. Add an A record set for mapping example.com to the IP address of the website.

    ii. Add CNAME record sets for mapping www.example.com to the domain names of the cloud services such as CDN, WAF, or OBS.

    iii. Configure 301/302 redirection for the website IP address to redirect example.com to www.example.com.

  - **Accessing a mailbox**: An MX record set and an A record set can coexist for the primary domain name example.com.

For details about how to add an A, CNAME, or MX record, see **Adding Record Sets**.

- (Not Recommended) Alternative Solution

  If 301/302 redirection cannot be configured and you want both a CNAME record set and an MX record set to be configured for the domain name, the office mailbox of your enterprise may become unavailable.

  If a local client first accesses the website using example.com, the domain name is mapped to www.example.com.c.cdnhwc1.com (domain name of CDN). The local DNS server caches the CNAME value based on the TTL. If at this time the local client accesses the mailbox, the MX record set configured for example.com is requested. Because the local DNS server has already cached the CNAME value of example.com, the local DNS directly returns www.example.com.c.cdnhwc1.com. As a result, the request to the MX record set fails. The email sending and receiving of the mailbox is affected and will restore only after the cache of the CNAME value expires.

  You can refer to the following configuration:

  – **Accessing a website**: Add a CNAME record set for example.com to map the domain name to the domain name of the cloud service such as CDN, WAF, or OBS.
  – **Accessing a mailbox**: Add an MX record set for example.com using a different line to avoid conflicts with the CNAME record set.

  WARNING

  This alternative solution works for record set conflicts but cannot prevent the situation where the mailbox may become unavailable. Evaluate the risks carefully.

Conflicts when Adding an NS Record Set

You have hosted domain name example.com on the DNS service. An NS record set and an SOA record set are automatically created for the hosted zone and cannot be deleted.

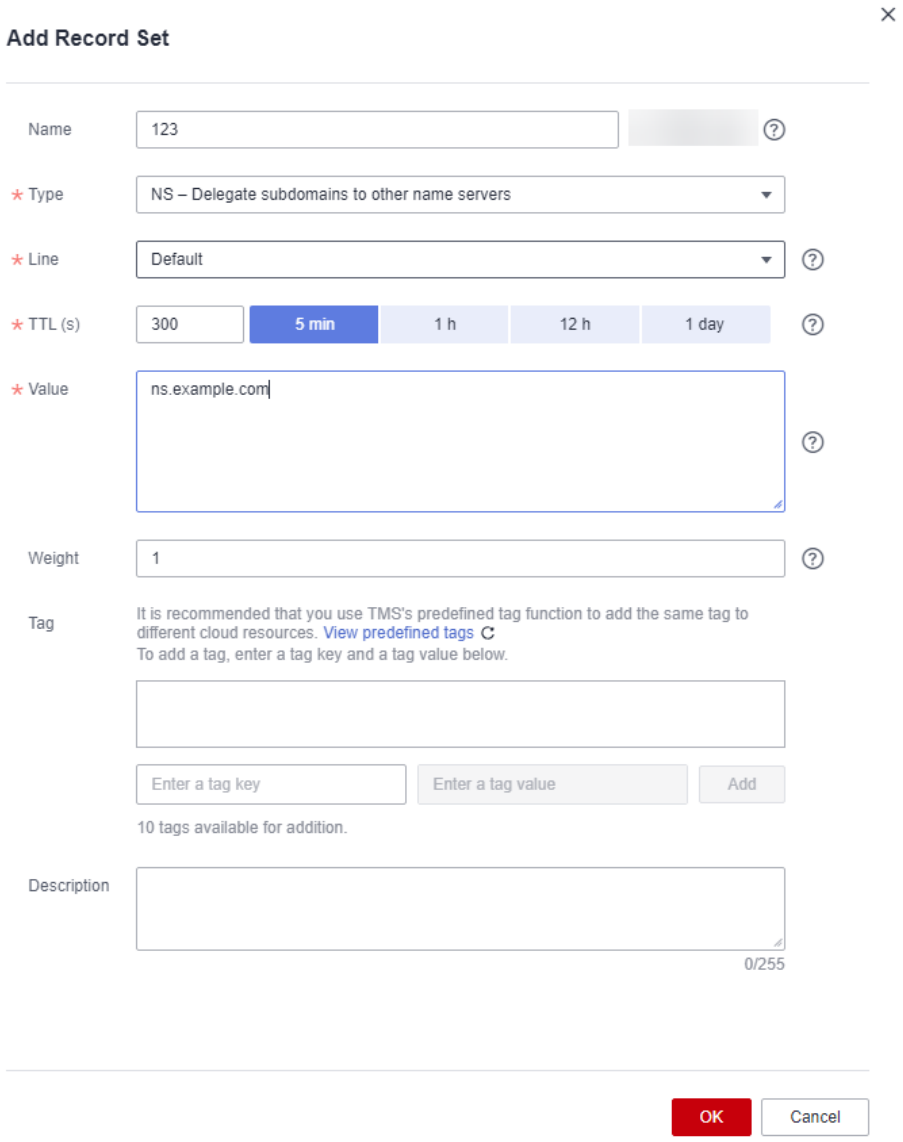
If the resolution line is the same, no NS record set can be added to the domain name example.com.

In this case, use either of the following methods to add a record set:

- **Method 1: Add an NS record set for a subdomain of the domain name.**

  In the following figure, an NS record set is added for 123.example.com, and the value of the record set is **ns.example.com**.

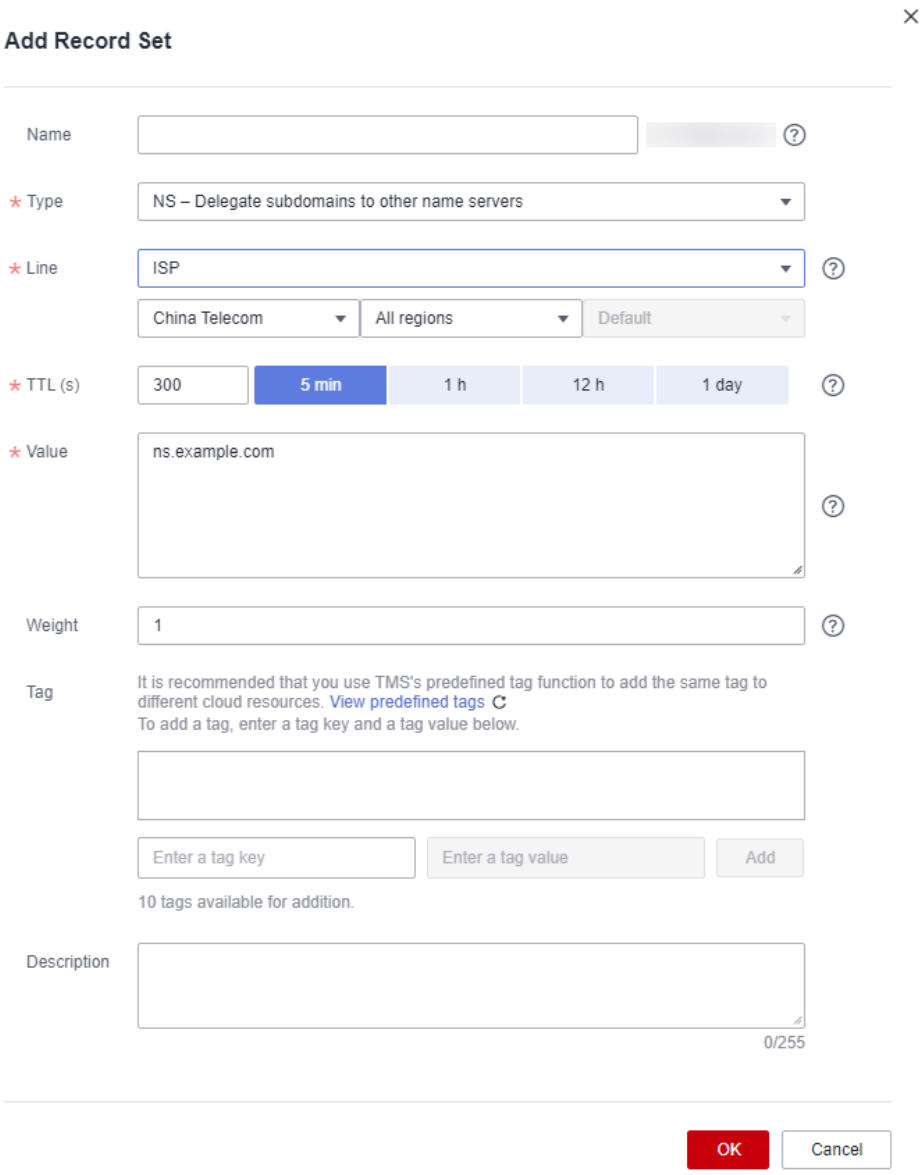
Figure 2-9 Adding an NS record set



- **Method 2: Add an NS record set to example.com, with a resolution line other than the default line.**

  In the following figure, an NS record set with the line type set to **ISP** is added for example.com, and the value of the record set is ns.example.com.

Figure 2-10 Adding an NS record set with an ISP line



- **Method 3: Change the value of the NS record set added to example.com.**

  For details, see **Modifying a Record Set**.

  To configure a new authoritative DNS server address for a domain name, modify the value of the NS record set added to the hosted zone. For details, see **What Are Huawei Cloud DNS Servers?**

Other Conflicts

If message "This record set is in conflict with an existing one" is displayed, perform either of the following operations if you still want to add a record set.

- Add a record set of a different name for a subdomain of the domain name.
- Add a record set of a different line type. Select a line other than **Default**.
- Delete the record set that conflicts with others and then add another one.

> **WARNING**
>
> Deleting a record set may cause domain name resolution to fail.

2.4 Record Sets

2.4.1 Overview

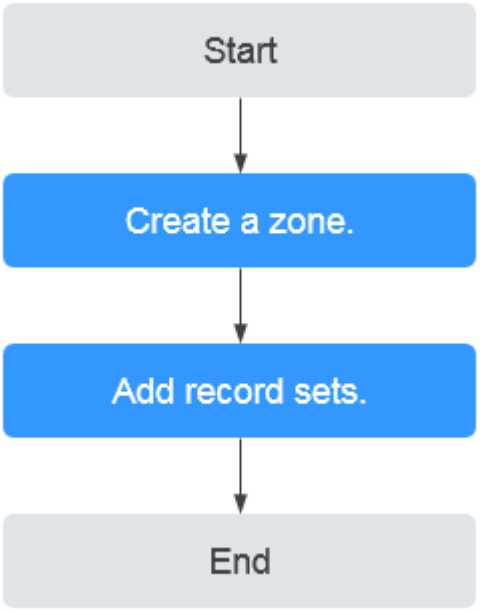
What Is a Record Set?

A record set translates a domain name into an IP address or other related information during DNS resolution. It defines the mapping between domain names and servers or other resources to ensure that users can find the corresponding network services when accessing domain names.

Process for Configuring a Record Set

Figure 2-11 shows the process for configuring a record set on the DNS console.

Figure 2-11 Process for configuring a record set



Related Operations

Operation	Description
Adding Record Sets for a Public Zone	Configure record sets for public zones.

Operation	Description
Managing Record Sets	Modify a record set, delete a record set, batch delete record sets in a single zone, and view record set details.
Managing Record Sets in Batches	Add, modify, and delete record sets in batches.
Disabling or Enabling Record Sets	Disable or enable record sets for a domain name. SOA and NS record sets are automatically generated and cannot be disabled.
Configuring a Wildcard DNS Record Set	Map all subdomains of a domain name to the same value. SOA and NS record sets are automatically generated and cannot be disabled.
Configuring Weighted Routing	Set weights for different record sets for load balancing, failover, and leveraging geographical location benefits. • You can configure weights for up to 20 record sets of the same domain name and line. • If the weight of a record set is set to 0, no result will be returned.

2.4.2 Adding Record Sets for a Public Zone

Scenarios

After creating a public zone for your domain name, you need to add record sets for your zone. DNS supports multiple types of record sets that apply to different service scenarios.

Record Set Type	Where to Use
A	An A record set maps domain names to IPv4 addresses of website servers. If you want to make your website accessible via a domain name, you need to add an A record set to map the domain name to the IPv4 address of your web server.
CNAME	A CNAME record set is used for scenarios like website resolution, CDN, enterprise mailbox, enterprise portal, web application firewall, object storage, and live video streaming. It maps one domain name to another domain name or multiple domain names to one domain name.

Record Set Type	Where to Use
MX	An MX record set maps domain names to email servers. It is used for routing traffic to a mailbox. It records the email server's priority and host name.
AAAA	An AAAA record set maps domain names to IPv6 addresses of website servers.
TXT	A TXT record set is used as a digital authentication certificate and for SPF (anti-spam) and domain name retrieval. It creates text records for domain names.
SRV	An SRV record set records the services provided by servers, guiding clients to the correct server. It is commonly used for directory management at Microsoft.
NS	An NS record set is created by default. It specifies authoritative DNS servers of domain names. If you need to delegate a subdomain to a third-party DNS provider, you need to manually create an NS record for the subdomain.
SOA	An SOA record set provides basic information about domain names and details about authoritative servers. This type of record set is created by default and cannot be added manually.
CAA	Grants certificate issuing permissions to certificate authorities (CAs). CAA record sets can prevent the issuance of unauthorized HTTPS certificates.

This section describes how to add a record set for a public zone and the service scenarios and configuration rules of different types of record sets.

Preparations

- **Prepare a domain name.**

  You have purchased a domain name from the domain name registrar and added it to the DNS console. For details, see **Creating a Public Zone**.

- **The domain name is normal.**

  You have queried the domain name status from the domain name registrar or a third-party platform and confirmed that the domain name is in a normal status.

- **The DNS server address is correct.**

  After adding the domain name to the DNS console, check its DNS server address in the list and ensure that the Huawei Cloud DNS server address is used.

If the DNS server addresses of the domain name do not contain the Huawei Cloud DNS server address, add the Huawei Cloud DNS server address for it. For details, see **Changing DNS Servers for a Public Domain Name**.

- **You have obtained the value of the record set.**
  - To configure a record set for a website, you need to obtain the public IP address of the website server.
  - To configure a record set for cloud services such as CDN, WAF, and OBS, you need to obtain the CNAME values provided by the cloud services.
  - To configure an email domain name, you need to obtain the MX record provided by the email service provider.

Adding a Record Set

A Records

An A record set maps a domain name to an IPv4 address. If you have a website with a public IP address and domain name, you can map the domain name to the public IP address by adding an A record set. After the record set is added, the website can be accessed using the domain name.

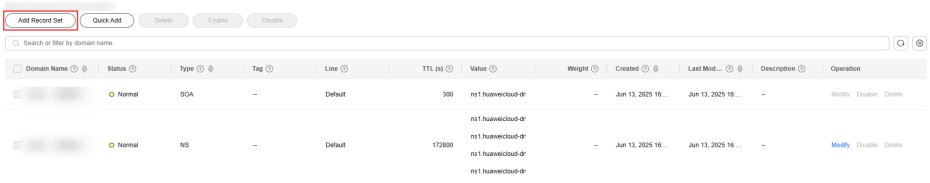
Constraints

An A record cannot coexist with a CNAME, explicit URL, or implicit URL record for the same name and line.

For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Public Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.
3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

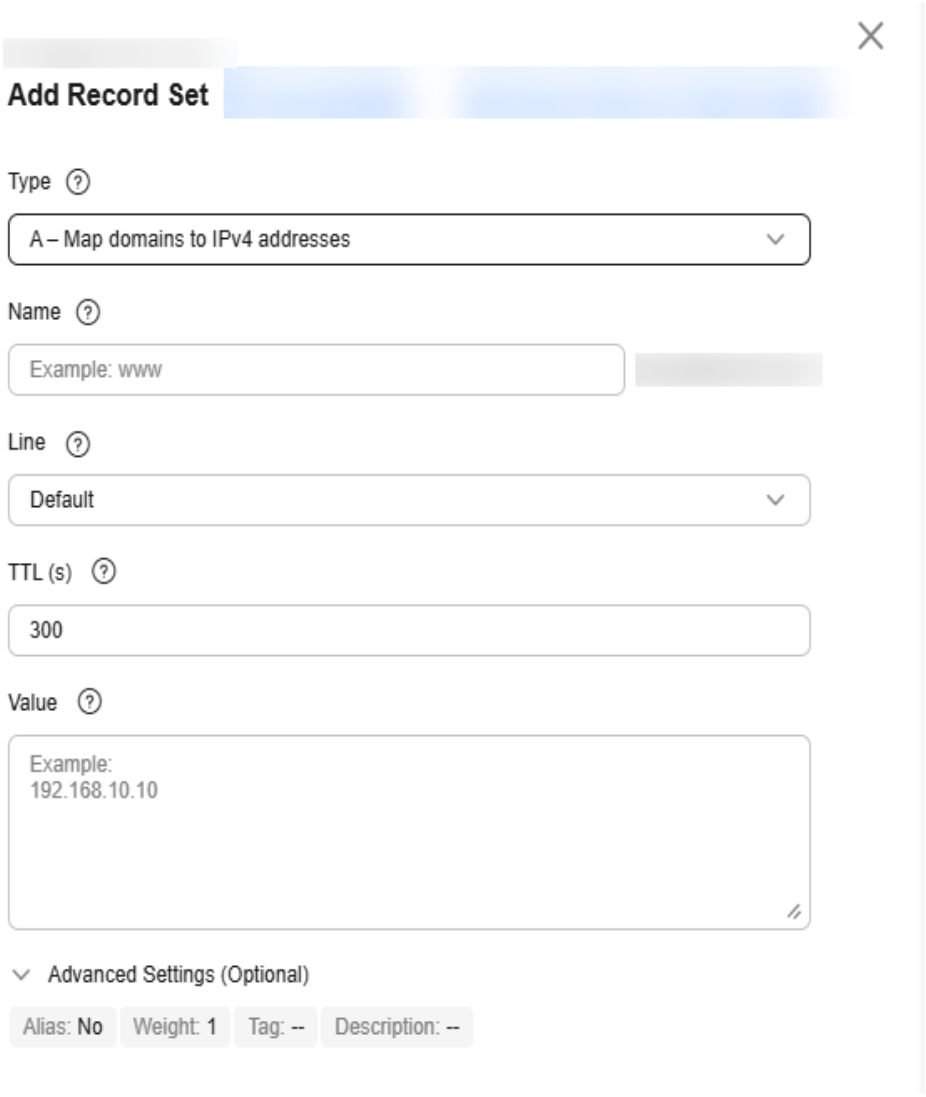


Table 2-8 Record set parameters

Parameter	Description	Example
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**.	A – Map domains to IPv4 addresses

Parameter	Description	Example
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default

Parameter	Description	Example
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300
Value	Record set value, which is usually the public IP address of a website server. You can enter a maximum of 50 unique IP addresses, each on a separate line.	198.xx.xx.100 198.xx.xx.101 198.xx.xx.102
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1

Parameter	Description	Example
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Routing Internet traffic to a website

5. Click **OK**.

CNAME Records

A CNAME record maps a domain name to another. It is commonly used for domain name resolution of CDN, WAF, OBS buckets, and EWP. You can also use CNAME records to map a subdomain name (for example, starting with www.) to the primary domain name.

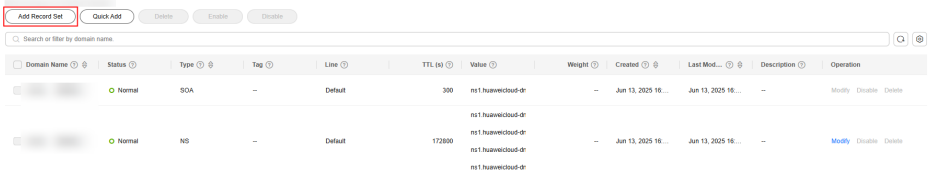
Constraints

A CNAME record cannot coexist with other types of records for the same name and line.

For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Public Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.
3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

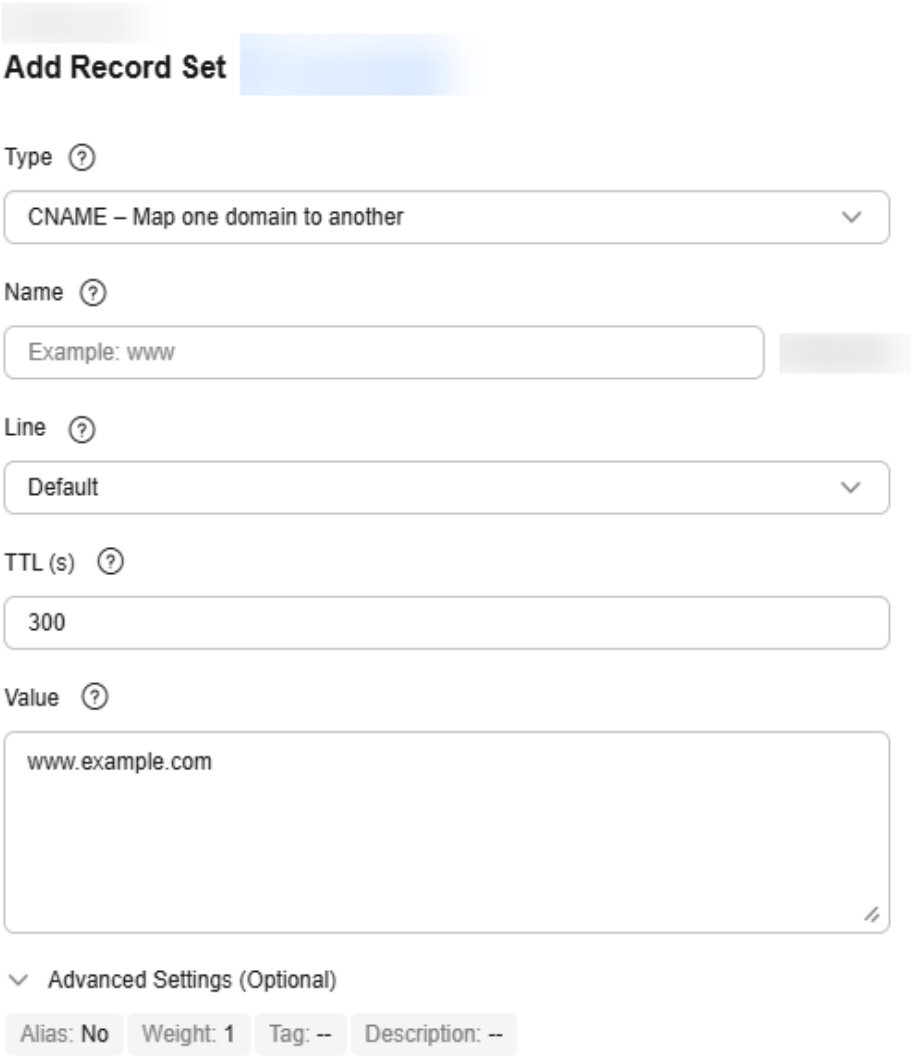


Table 2-9 Record set parameters

Parameter	Description	Example
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**.	CNAME – Map one domain to another
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.

Parameter	Description	Example
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300
Value	The domain name returned for DNS resolution, which is usually another domain name that maps the target IP address. You can enter a maximum of 50 unique IP addresses, each on a separate line.	www.example.com
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1

Parameter	Description	Example
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Routing Internet traffic to a website

5. Click **OK**.

MX Records

A Mail Exchange (MX) record set is used to specify the mail server that handles emails from a specific domain name. When an email system sends an email, it searches for the desired MX record based on the domain name in the recipient address to determine the location of the target mail server, ensuring that the email can be correctly sent to the target server. An MX record set contains the addresses and priorities of multiple mail servers to ensure the reliability and efficiency of email transmission.

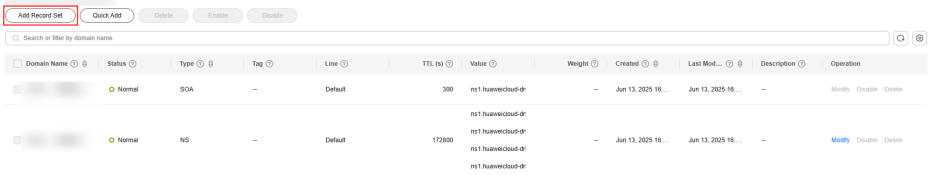
Constraints

An MX record cannot coexist with a CNAME, explicit URL, or implicit URL record for the same name and line.

For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Public Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.
3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

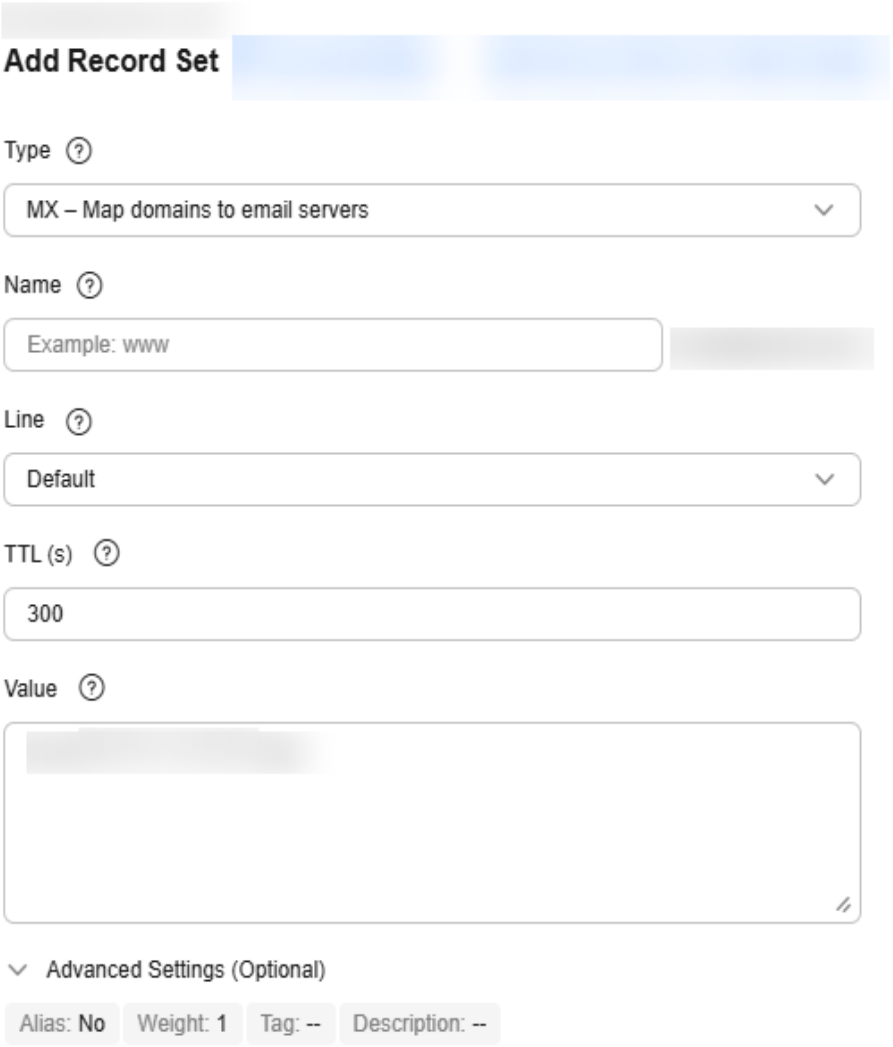


Table 2-10 Record set parameters

Parameter	Description	Example
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**.	MX – Map domains to email servers
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.

Parameter	Description	Example
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300
Value	Enter email server addresses. You can enter a maximum of 50 unique addresses, each on a separate line. The format is *[priority][mail-server-host-name]*. **Configuration rules:** • **priority**: priority for an email server to receive emails. A smaller value indicates a higher priority. • **mail server host name**: domain name provided by the email service provider	10 mailserver.example.com.

Parameter	Description	Example
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Email domain name resolution

5. Click **OK**.

AAAA Records

An AAAA record is used to map a domain name to an IPv6 address. It is used for domain name resolution when websites support IPv6 addresses. If you have a

website with a public IPv6 address and domain name, you can map the domain name to the IPv6 address by adding an AAAA record set. After the record set is added, the website can be accessed using the domain name.

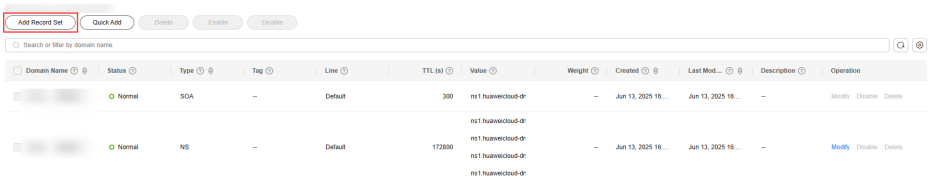
Constraints

An AAAA record cannot coexist with a CNAME, explicit URL, or implicit URL record for the same name and line.

For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Public Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.
3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

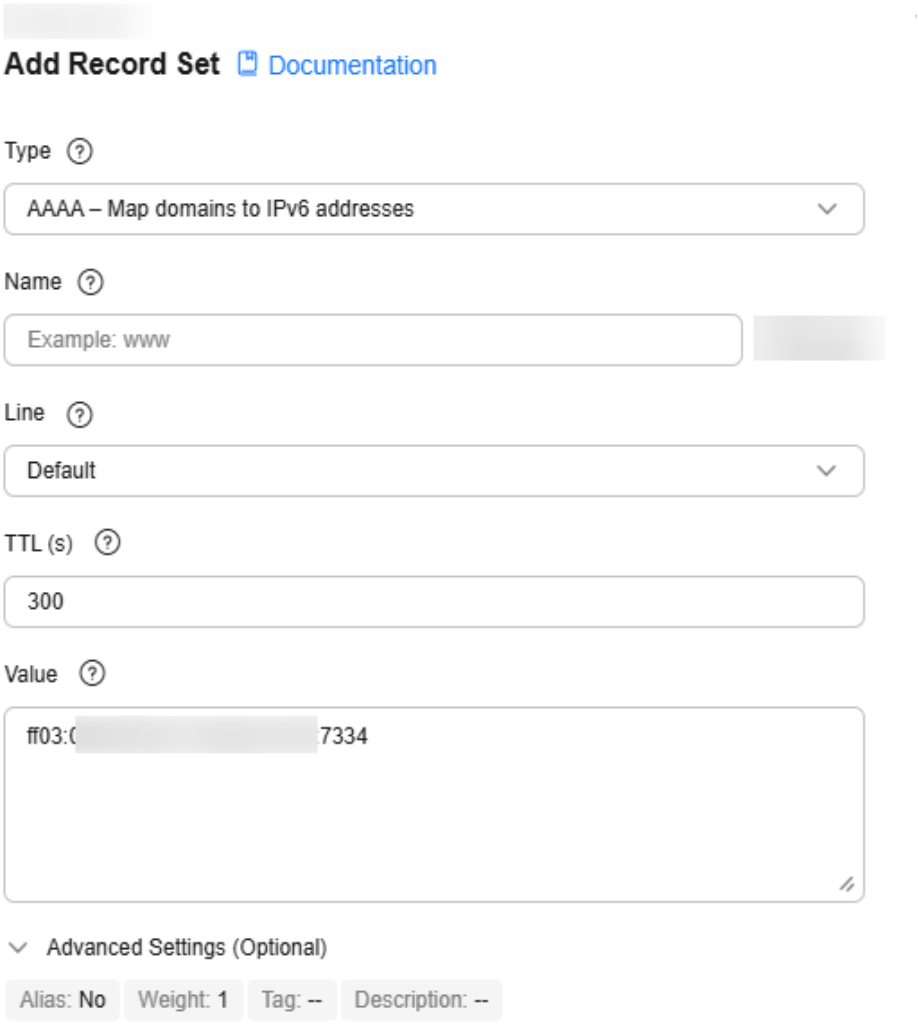


Table 2-11 Record set parameters

Parameter	Description	Example
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**.	AAAA – Map domain names to IPv6 addresses

Parameter	Description	Example
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default

Parameter	Description	Example
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300
Value	IPv6 addresses mapped to the domain name. You can enter a maximum of 50 unique IP addresses, each on a separate line.	ff03:0db8:85a3:0:0:8a2e:0370:7334
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1

Parameter	Description	Example
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1
Description	Supplementary information about the record set. Can contain a maximum of 255 characters.	IPv6 address type

5. Click **OK**.

TXT Records

A TXT record is used to identify and describe a domain name. It is usually used for configuring SPF (anti-spam), DKIM (email signature), and verifying the domain name ownership.

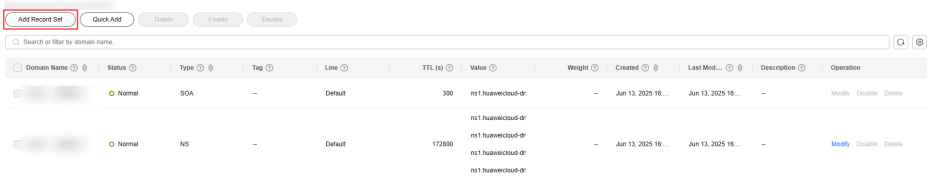
Constraints

A TXT record cannot coexist with a CNAME, explicit URL, or implicit URL record for the same name and line.

For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Public Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.
3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

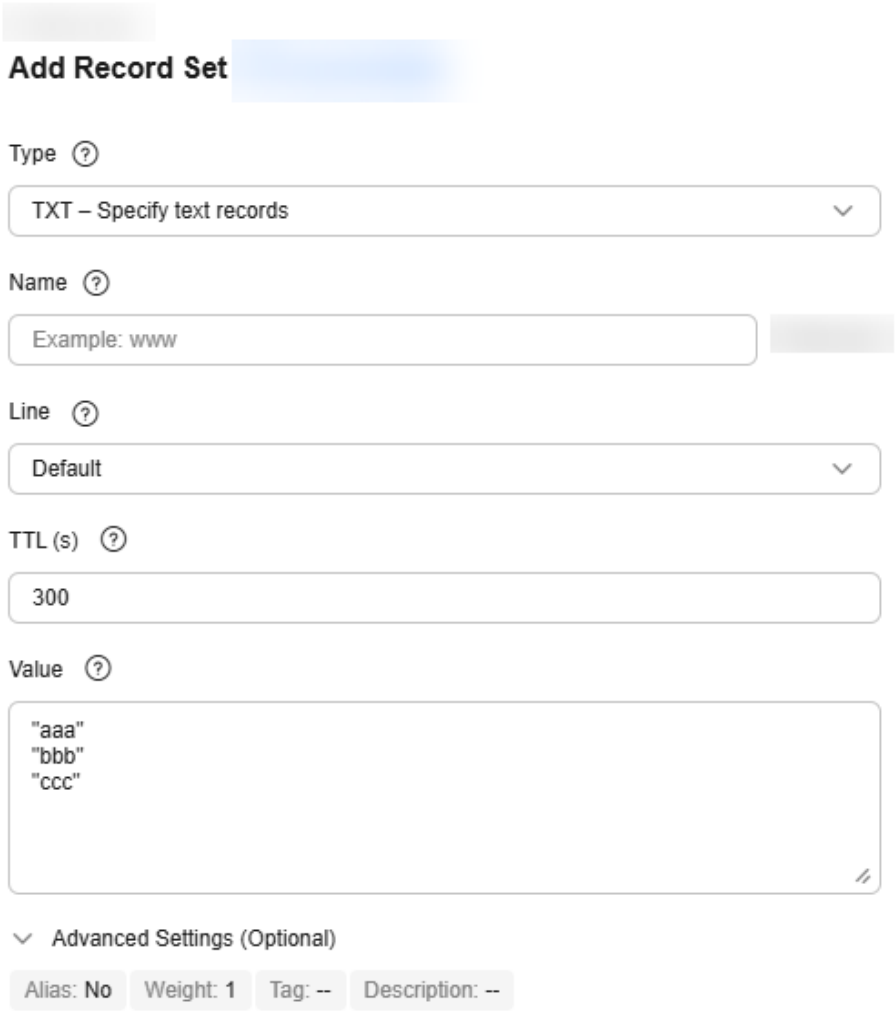


Table 2-12 Record set parameters

Parameter	Description	Example
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**.	TXT – Specify text records
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.

Parameter	Description	Example
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300

Parameter	Description	Example
Value	Enter text content as required. 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 4,096 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" • Text record in SPF format: "v=spf1 a mx -all" Only IP addresses in the A and MX record sets are authorized to send emails using this domain name.
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1

Parameter	Description	Example
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1
Description	Supplementary information about the record set. Can contain a maximum of 255 characters.	TXT record set

5. Click **OK**.

SRV Records

An SRV record is used to identify the services provided by a cloud server. It usually applies to VoIP, instant messaging, and email to provide load balancing, failover, and automatic service discovery.

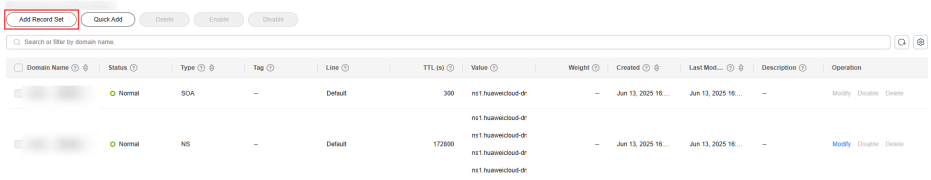
Constraints

An SRV record cannot coexist with a CNAME, explicit URL, or implicit URL record for the same name and line.

For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Public Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.
3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

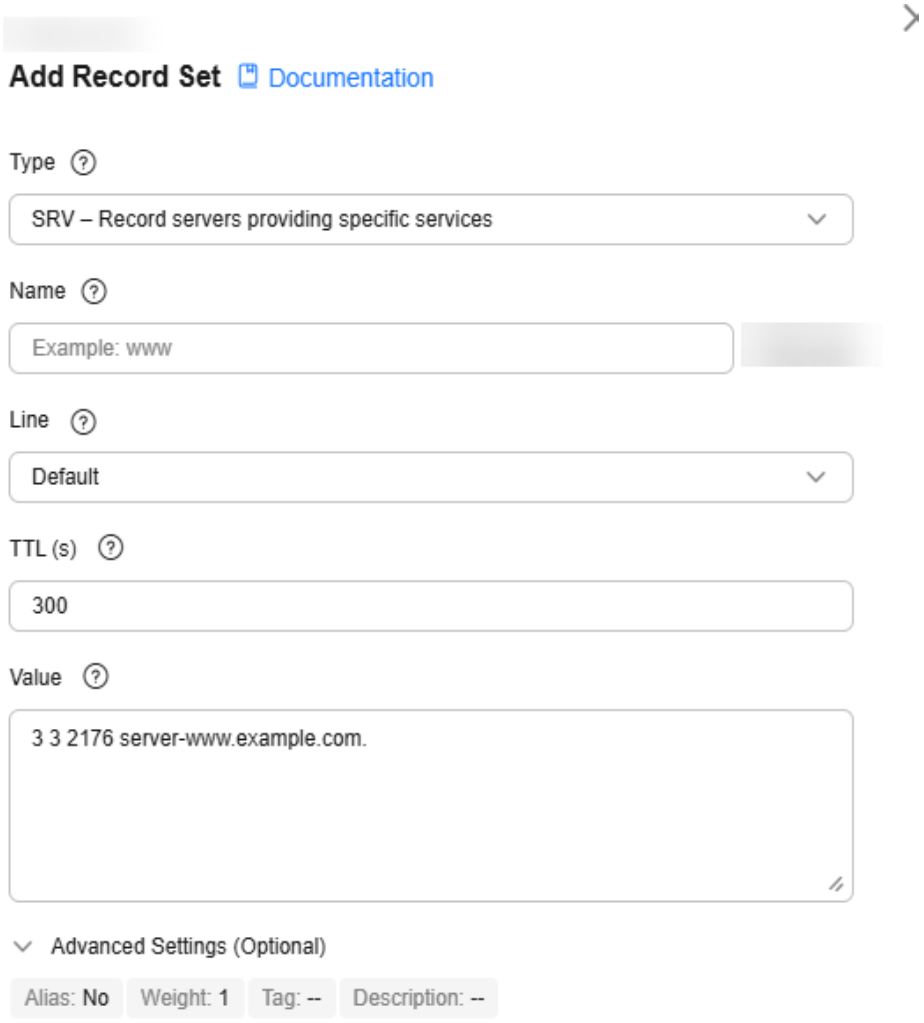


Table 2-13 Record set parameters

Parameter	Description	Example
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**.	SRV – Record servers providing specific services
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.

Parameter	Description	Example
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300

Parameter	Description	Example
Value	Enter the specific server address. You can enter a maximum of 50 unique addresses, each on a separate line. The value format is *[priority] [weight] [port] [server host name]*. **Configuration rules:** • The priority, weight, and port number range from 0 to 65535. • A smaller value indicates a higher priority. • A larger value indicates a larger weight. • The host name is the domain name of the target server. **NOTE** If the record set values have the same priority, requests to the domain name will be routed based on weights.	3 3 2176 server-www.example.com
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1

Parameter	Description	Example
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: ● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 128 characters. ● Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: ● Can be left blank. ● Can contain a maximum of 255 characters. ● Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1
Description	Supplementary information about the record set. Can contain a maximum of 255 characters.	SRV record set

5. Click **OK**.

NS Records

An NS record specifies authoritative DNS servers for a domain name. If you want to delegate a subdomain to other DNS service providers, you can add an NS record for the subdomain.

Constraints

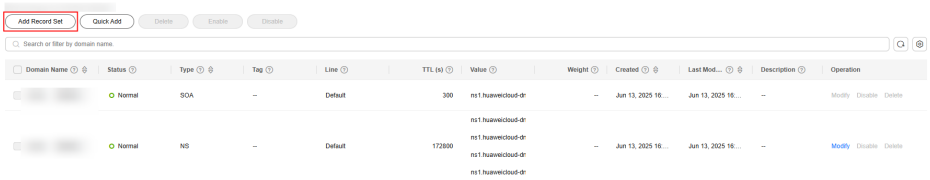
After a public zone is created, an NS record set is automatically created for this zone and cannot be deleted. You can add NS record sets only in the following scenarios:

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

If a conflict occurs when you add an NS record, handle it by referring to **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Public Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.
3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

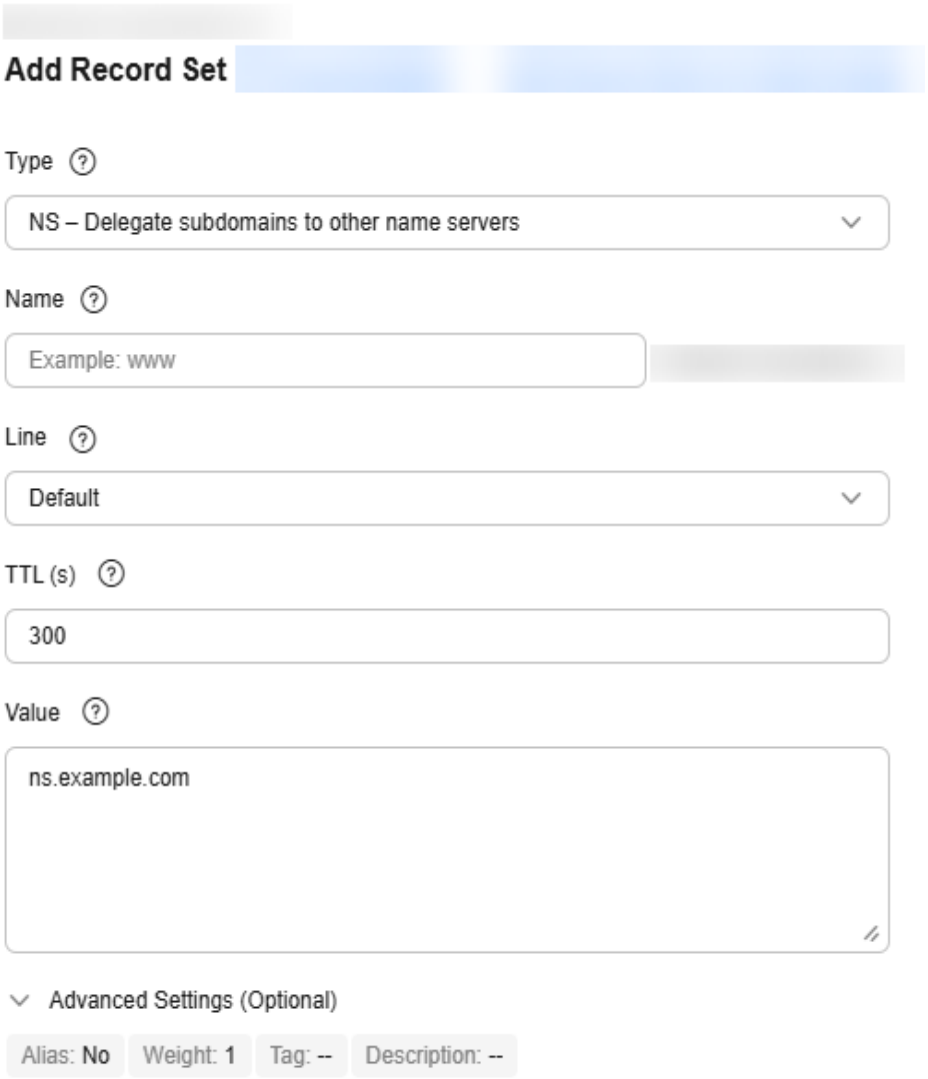


Table 2-14 Record set parameters

Parameter	Description	Example
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**.	NS – Delegate subdomains to other name servers
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	www

Parameter	Description	Example
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300
Value	Enter the addresses of the domain name servers to be authorized. You can enter a maximum of 50 unique addresses, each on a separate line.	ns.example.com
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1

Parameter	Description	Example
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1
Description	Supplementary information about the record set. Can contain a maximum of 255 characters.	NS record added for a subdomain

5. Click **OK**.

CAA Records

A CAA record specifies the CA that issues HTTPS certificates for a domain name to prevent incorrect certificate issuing.

Constraints

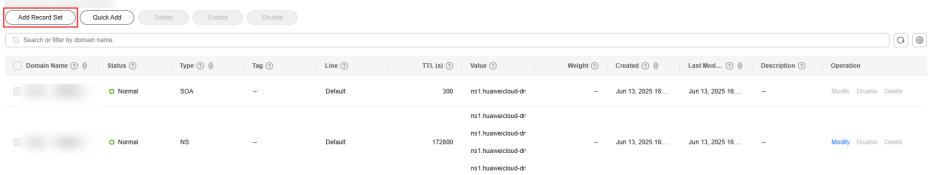
A CAA record cannot coexist with a CNAME, explicit URL, or implicit URL record for the same name and line.

For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Public Zones** page.

2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.
3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

Table 2-15 Record set parameters

Parameter	Description	Example
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**.	CAA – Grant certificate issuing permissions to CAs
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.

Parameter	Description	Example
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300

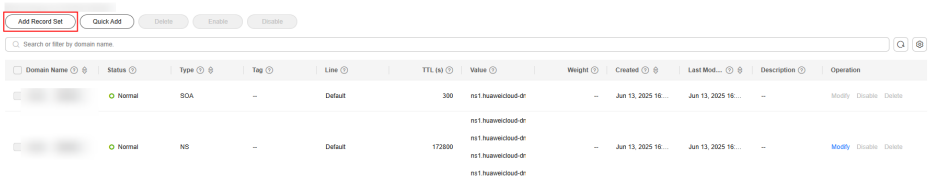
Parameter	Description	Example
Value	CA to be authorized to issue certificates for a domain name or its subdomains. You can enter a maximum of 50 different CAs, each on a separate line. The format is *[flag] [tag] [value]*. **Configuration rules:** • **flag**: CA identifier, an unsigned character ranging from 0 to 255. Usually, the value is set to **0**. • **tag**: You can enter 1 to 15 characters. Only letters and digits from 0 to 9 are allowed. The tag can be one of the following: – **issue**: authorizes a CA to issue all types of certificates. – **issuewild**: authorizes a CA to issue wildcard certificates. – **iodef**: requests notifications once a CA receives invalid certificate requests. • **value**: authorized CA or email address/URL required for notification once the CA receives invalid certificate requests. The value depends on the value of **tag** and must be enclosed in quotation marks (""). The value can contain a maximum of 255 characters. Only letters, digits, spaces, and the following special characters are allowed: -#*?&_~=:;.@+^/!%	0 issue "ca.abc.com" 0 issuewild "ca.def.com" 0 iodef "mailto:admin@domain.com" 0 iodef "http://domain.com/log/"

Parameter	Description	Example
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1
Description	Supplementary information about the record set. Can contain a maximum of 255 characters.	CAA record set

5. Click **OK**.

1. Go to the **Public Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.

3. Click **Add Record Set** above the record set list.



2.4.3 Managing Record Sets

Scenarios

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

Modifying a Record Set

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

NOTE

- You can modify the TTL, value, and description of the NS record set.
- SOA record sets are automatically generated and cannot be modified.

1. Go to the **Public Zones** page.
2. In the zone list, locate the zone and click the domain name.
3. Locate the record set you want to modify and click **Modify** in the **Operation** column.
4. Modify the parameters.

   You can change the name, type, TTL, value, weight, and description of a record set.

   For more details, see **Adding Record Sets for a Public Zone**.
5. Click **OK**.

Deleting a Record Set

You can delete a record set if it is no longer needed.

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

WARNING

Deleted record sets cannot be recovered, and domain name queries will fail. Exercise caution when performing this operation.

1. Go to the **Public Zones** page.
2. In the zone list, locate the zone and click the domain name.
3. Locate the record set you want to delete and click **Delete** in the **Operation** column.

4. In the displayed dialog box, confirm the record set to be deleted.

   Enter **DELETE** and click **OK**.

Viewing Details About a Record Set

1. Go to the **Public Zones** page.
2. In the zone list, locate the zone and click the domain name.
3. Locate the record set and view the details.

2.4.4 Managing Record Sets in Batches

Overview

DNS provides the batch operation function to facilitate efficiency in managing record sets.

It provides the following functions:

- **Adding Record Sets to Multiple Public Zones**: Add record sets of the same type for multiple zones and subdomains in batches in the same resolution line.
- **Deleting Record Sets from Multiple Public Zones**: Delete record sets with a specific name from multiple zones.
- **Modifying Record Sets**: Batch modify the names and values of record sets.
- **Exporting Record Sets**: Batch export all record sets of in a single zone.
- **Importing Record Sets**: Batch import record sets for a single zone.

Adding Record Sets to Multiple Public Zones

Scenario

DNS allows you to perform batch operations on record sets. You can add record sets of the same type for multiple zones and subdomains in batches in the same resolution line.

Table 2-16 provides some examples to describe how to add record sets for multiple domain names.

Table 2-16 Batch adding record sets

Domain Name	Record Set Name	Record Set Type	Value	Description
exampletest1.com	-	A	192.168.1.1	Add an A record set to domain name exampletest1.com to map it to 192.168.1.1.

Domain Name	Record Set Name	Record Set Type	Value	Description
	123			Add an A record set to subdomain 123.exampletest1.com to map it to 192.168.1.1.
	www			Add an A record set to subdomain www.exampletest1.com to map it to 192.168.1.1.
exampletest2.com	-	A		Add an A record set to domain name exampletest2.com to map it to 192.168.1.1.
	123			Add an A record set to subdomain 123.exampletest2.com to map it to 192.168.1.1.
	www			Add an A record set to subdomain www.exampletest2.com to map it to 192.168.1.1.
exampletest3.com	-	A		Add an A record set to the domain name exampletest3.com to map the domain name to 192.168.1.1.
	123			Add an A record set to subdomain 123.exampletest3.com to map it to 192.168.1.1.
	www			Add an A record set to subdomain www.exampletest3.com to map it to 192.168.1.1.

Constraints

- You can only add record sets to public zones in batches.
- Before you add record sets, you must have created public zones by following the instructions in **Creating a Public Zone**, or the added record sets will not take effect.
- When you add record sets, note the following:
  - You can add record sets to up to 10,000 public zones at a time.

- Up to 10 record sets can be added to each zone (including the subdomains).
- The record set name is the same for each zone.
- The line type is set to **Default**.
- The TTL is set to 300s by default.

Procedure

1. Go to the **Public Zones** page.
2. Select the zones to which you want to add record sets and select **Add Record Sets** from the **Batch Operations** drop-down list.
3. On the **Add Record Sets** page, configure the parameters based on **Table 2-16**.
   - **Domain Name**: domain names that you want to configure record sets for.

     NOTE

     - You do not need to set this parameter since you have already selected the zones in 2.
     - If you click **Add Record Sets** without selecting any zones, enter the domain names, with each on a separate line.
   - **Type**: type of record set to be added
   - **Record Set Name**: prefix for the domain names
   - **Value**: value of the record sets
4. Click **Submit**.

   After the operation is complete, you can view the operation name, result, time, and status on the **View Batch Operations** tab. You can also download failed operations.

Deleting Record Sets from Multiple Public Zones

Scenario

You can delete record sets with a specific name from multiple zones in batches.

WARNING

Deleted record sets cannot be recovered, and domain name queries will fail. Exercise caution when performing this operation.

Table 2-17 provides some examples to describe how to delete record sets from multiple zones.

Table 2-17 Deleting record sets

Domain Name	Record Set Name	Description
exampletest1.com	-	Deletes all record sets of domain name exampletest1.com.

Domain Name	Record Set Name	Description
	123	Deletes all record sets of domain name 123.exampletest1.com.
exampletest2.com	-	Deletes all record sets of domain name exampletest2.com.
	123	Deletes all record sets of domain name 123.exampletest2.com.
exampletest3.com	-	Deletes all record sets of domain name exampletest3.com.
	123	Deletes all record sets of domain name 123.exampletest3.com.

Constraints

- Only record sets added to public zones can be deleted in batches.
- SOA and NS record sets are automatically generated and cannot be deleted.
- If specified record sets do not exist for a domain name, these record sets will not be deleted.
- When deleting record sets, note the following:
  - You can delete record sets from no more than 10,000 domain names at a time.
  - Up to five record set names can be modified at a time.

Procedure

1. Go to the **Public Zones** page.
2. Select the zones from which you want to delete record sets, and select **Delete Record Sets** from the **Batch Operations** drop-down list.
3. On the **Delete Record Sets** page, configure the parameters based on **Table 2-16**.
   - **Domain Name**: domain names whose record sets you want to delete

     NOTE

     - You do not need to set this parameter since you have already selected the zones in 2.
     - If you click **Delete Record Sets** without selecting any zones, enter the domain names, with each on a separate line.
   - **Deletion Condition**: **Delete record sets meeting any of the conditions** is selected by default.

     Currently, **Record set name** is the only deletion condition.
4. Click **Submit**.

   After the operation is complete, you can view the operation name, result, time, and status on the **View Batch Operations** tab. You can also download failed operations.

Modifying Record Sets

Scenario

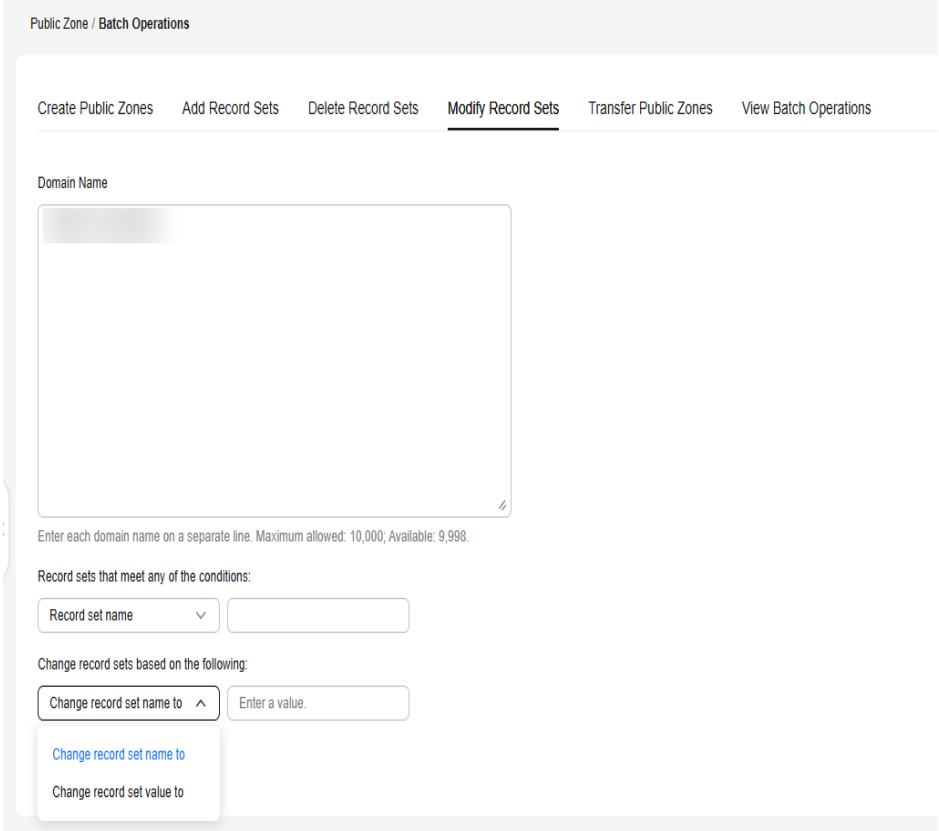
You can modify the name or value of the record sets configured for multiple domain names in batches.

Constraints

- Only record sets added to public zones can be modified in batches.
- Only A record sets can be modified.
- Either the name or value of the record sets can be modified. They cannot be modified at the same time.
- When modifying record sets, note the following:
  - You can modify record sets to no more than 10,000 domain names at a time.
  - Up to five record set names can be modified at a time.
  - Up to 50 unique record set values are allowed.

Procedure

1. Go to the **Public Zones** page.
2. In the public zone list, select the zone whose record sets are to be modified.
3. In the upper part of the public zone list, choose **Batch Operations** > **Modify Record Sets**.
4. On the displayed page, configure the parameters as prompted.
   - **Domain Name**: The selected domain names are displayed by default. You can also enter the domain names. Enter each domain name on a separate line. Up to 10,000 domain names can be entered.
   - **Record set name**: Enter the new name for the record sets. You can enter up to five record set names. Each time you enter a record set name and press **Enter**.
   - **Record sets that meet any of the conditions**: Modify the record set name or value.
     - **Change record set name to**: Enter a new record set name. If you select this option, you cannot configure new record set values.
     - **Change record set value to**: Enter a new IP address on each line. You can enter up to 50 different IP addresses. If you select this option, you cannot need to configure new record names.



5. Click **Submit**.

   After the operation is complete, you can view the operation name, result, time, and status on the **View Batch Operations** tab. You can also download failed operations.

Exporting Record Sets

Scenario

If you want to transfer your domain name to another cloud service provider, you can export all the record sets configured for the domain name in batches.

You can export the following information about a public zone record set: record set name, record set type, line type, TTL (s), weight, record set value, status, description, record set ID, time when the record set was created, and time when the record set was last modified.

Procedure

1. Go to the **Public Zones** page.
2. In the public zone list, click the name of the public zone whose record sets are to be exported.
3. Click the **Export and Import** tab.
4. Click **Export Record Set** in the upper right corner of the page.

   An .xlsx file named using the domain name is exported, for example, **example.com.xlsx**.

   In the exported file, you can view the following information about a record set: record set name, record set type, line type, TTL (s), weight, record set

value, status, description, record set ID, time when the record set was created, and time when the record set was last modified.

Importing Record Sets

Scenario

If you want to transfer your domain name from another cloud server provider to the DNS service for hosting, you can import existing record sets configured for the domain name in batches.

You can import up to 500 record sets at a time.

NOTE

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

Procedure

1. Go to the **Public Zones** page.
2. In the public zone list, click the name of the public zone to which record sets are to be imported.
3. Click the **Export and Import** tab.
4. Before you import record sets, list them as required in the template.
   a. Click **Download template** in the note.
   b. Fill in the template as required.

      NOTE

      If you have exported record sets from the previous service provider, you need to fill them in the template. If the format is incorrect, the import may fail.
5. In the upper right corner of the page, click **Import Record Set** and select the record set file to import.

   You can check whether record sets are imported or not.

   - **Successful Import**: The number of successfully imported record sets are displayed.
   - **Failed Import**: All failed record sets are listed. You can resolve the problems based on the causes.

     NOTE

     Before importing record sets again, click **Clear** in the upper right corner of the page to clear both the record sets that have been imported successfully and the record sets failed to be imported.

Helpful Links

Common issues and solutions for failures in batch importing record sets

Error Message	Possible Causes	Solution
There is already an import task for this domain name. Clear the existing task and then continue the import.	The record sets that failed to be batch imported were not cleared.	Click **Clear** in the upper right corner of the **Export and Import** tab and try again.
Invalid record set types. Only A, CAA, AAAA, MX, CNAME, TXT, and NS record sets are allowed.	The types of the record sets to be imported are invalid.	Modify or delete the record sets of invalid types and try again.
The record set weight must range from 0 to 1,000.	Weight of the record set attempted to be imported is not from 0 to 1000.	Change the record set weight to a proper value and try again. Value range: **0** to **1000**
Invalid record set value.	The values of the record sets to be imported are invalid.	Modify the record set values as needed and try again. For details, see **Record Set Types and Configuration Rules**.
The resolution line does not exist.	The resolution line of the record set attempted to be imported does not exist.	Modify the resolution line of the record set and try again. Enter different resolution lines in the following format: • **Default**: Select **Default**. • **ISP**: Select a line, for example, China Telecom, China Telecom_North China, and China Telecom_Beijing. For details, see **ISP Lines**. • **Region**: Select Chinese Mainland, Chinese mainland_North China, Chinese mainland_Beijing or other options. For details, see **Region Lines**.
Domain name configured in the record set must be valid.	Invalid domain name configured in the record set.	Enter **www** for the **Name** field or leave it blank. You can also enter **www.example.com.** (a domain name with a period at the end) for the **Name** field.

Error Message	Possible Causes	Solution
Invalid zone description. The description can contain up to 255 characters.	Invalid domain name configured in the record set.	Change the record set description to a proper value and try again. The value can contain a maximum of 255 characters.
Invalid TTL value.	TTL of the record sets attempted to be imported are invalid.	Change the record set TTL to a proper value and try again. Value range: **1** to **2147483647**

2.4.5 Disabling or Enabling Record Sets

Scenarios

You can disable a zone or its record sets on the DNS console. If you disable a zone or record set, it cannot be used for resolution. You can enable the zone or record set at any time if you need it again.

The domain name registry reviews the legitimacy of the website and forbids the access to the website during the domain name licensing. If you have added record sets on the DNS console, you need to disable them and then enable them after the licensing is complete.

This section describes how to disable or enable record sets.

Constraints

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

Disabling Record Sets

You can disable the record sets added to a public zone in the **Normal** state.

1. Go to the **Public Zones** page.
2. Disable record sets.
   - To disable all record sets added to a zone: Locate the zone and click **Disable** in the **Operation** column.
   - **Disabling a record set**: Locate the zone and click the domain name to go to the record set list. Locate the target record set, click **Disable** in the **Operation** column.
   - **Disabling multiple record sets**: Locate the zone and click the domain name to go to the record set list. Select the record sets, click **Disable** above the record set list.

   NOTE

   After a record set is disabled, it cannot be used for resolution, but you can view it in the record set list.

3. Click **OK**.

Enabling Record Sets

You can enable the record sets that have been disabled.

1. Go to the **Public Zones** page.
2. Enable record sets.
   - To enable all record sets added to a zone: Locate the zone and click **Enable** in the **Operation** column.
   - To enable one or more record sets: Click the domain name to go to the **Record Sets** tab. Locate each record set you want to enable and click **Enable** in the **Operation** column.
3. Click **OK**.

2.4.6 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.

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

Constraints

- Wildcard DNS resolution does not support NS and SOA record sets.
- Exact match has a higher priority than fuzzy match for the same domain name.

Procedure

1. Go to the **Public Zones** page.
2. Click the name of the zone to which you want to add a wildcard DNS record set.
3. Click **Add Record Set**.
4. Configure the parameters based on **Table 2-18**.

Table 2-18 Parameters for adding a wildcard DNS record set

Parameter	Description	Example
Type	Record set type Wildcard DNS resolution does not support NS and SOA record sets.	A – Map domains to IPv4 addresses

Parameter	Description	Example
Name	Public (or private) domain name Enter an asterisk (*) as the leftmost label of the domain name, for example, ***.example.com**. **NOTE** Only the leftmost asterisk is considered as a wildcard character. Other asterisks in the domain name are common text characters.	*
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300
Value	Returned result of domain name resolution. For details about how to configure the value for each type of record set, see **Table 2-5**.	The following uses an A record set as an example: 192.168.xx.2 192.168.xx.3

Parameter	Description	Example
Alias Target	Cloud resource to be associated with the alias record set, which includes the cloud resource name and alias target.	Enterprise Web Portal and example.com
Weight	Weight for the record set. Default value: **1** The value ranges from **0** to **1000**. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	This is a wildcard DNS record set.

5. Click **OK**.
6. Switch back to the **Record Sets** tab.
   The wildcard DNS record set in the **Normal** state.
   For details, see **How Do I Check Whether a Record Set Has Taken Effect?**

2.5 Intelligent Resolution

2.5.1 Intelligent Resolution Overview

Overview

Typically, a DNS server returns the same resolution result to visitors from different networks or geographical locations. However, in case of cross-network or cross-region access, this would lead to long latency and poor user experience.

With configurable resolution lines, you can specify that the DNS server return different resolution results for the same domain name based on the networks or geographical locations of visitors' IP addresses.

In addition to ISP and region lines, Huawei Cloud DNS allows you to customize resolution lines based on IP address ranges to route visitors to different web servers.

For a website deployed on multiple servers, you can set different weights for the record sets to balance the loads of these servers.

Where to Use

Table 2-19 describes the application scenarios of DNS Resolver.

Table 2-19 Application scenarios of DNS Resolver

Operation	Scenario
Configuring ISP Lines for Record Sets	Configure ISP lines to distinguish visitors by carrier.
Configuring Region Lines for Record Sets	Configure region lines to distinguish visitors by geographical location.
Configuring Custom Lines	Configure custom lines to distinguish visitors by IP address range.
Configuring Weighted Routing	Configure weight-based resolution for load balancing based on the proportion of requests to each record set.

2.5.2 Configuring ISP Lines

Background

Usually, a DNS server returns the same IP address to visitors from different networks. However, in cross-network access, this would lead to high latency and poor user experience.

If you configure ISP lines when you create record sets, the DNS server returns different resolution results or IP addresses to visitors based on their carrier networks.

For example, you have built a website using domain name example.com and hosted the website on three servers, with one in a China Telecom equipment room, one in a China Unicom data center, and one in a China Mobile data center. You need to configure four ISP lines: **Default**, **China Telecom**, **China Unicom**, and **China Mobile**.

Constraints

- ISP lines can be configured only for public zones.
- If a resolution line becomes faulty, you cannot switch to another resolution line.

ISP Lines

ISP lines are categorized by telecom carriers in China.

Table 2-20 ISP lines

Level 1	Level 2	Level 3
China Telecom, China Mobile, China Unicom, and Pengboshi	All regions	Default
	North China	Default, Beijing, Tianjin, Hebei, Shanxi, and Inner Mongolia
	Northeast China	Default, Liaoning, Jilin, and Heilongjiang
	Northwest China	Default, Shaanxi, Gansu, Qinghai, Ningxia, and Xinjiang
	Central China	Default, Henan, Hubei, and Hunan
	East China	Default, Shanghai, Jiangsu, Zhejiang, Anhui, Fujian, Jiangxi, and Shandong
	South China	Default, Guangdong, Hainan, and Guangxi
	Southwest China	Default, Chongqing, Sichuan, Guizhou, Yunnan, and Xizang

Level 1	Level 2	Level 3
Jiaoyuwang and Tietong	All regions	Default

For example, you have configured the following resolution lines for example.com:

- **Default**: 1.1.1.1
- **China Telecom**: 2.2.2.2
- **China Telecom_North China**: 3.3.3.3

When a China Telecom user in North China requests the domain name example.com, IP address 3.3.3.3 is returned. When a China Telecom user in another region requests this domain name, IP address 2.2.2.2 is returned. When a non-China Telecom user in a region other than North China requests the domain name, IP address 1.1.1.1 is returned.

Procedure

Configure ISP lines for your public domain names hosted on the DNS service.

The following describes how to configure a **Default** line to map the domain name to 1.1.1.1 and a **China Telecom** line to map the domain name to 2.2.2.2.

1. Go to the **Public Zones** page.
2. On the **Public Zones** page, click the domain name (**example.com**) of the public zone.
3. Click **Add Record Set**.
4. Add two A record sets for example.com. Configure the parameters based on **Table 2-21**.

Table 2-21 Parameters for adding an A record set

Parameter	Description	Line 1	Line 2
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**. An A record set is selected here.	A – Map domains to IPv4 addresses	A – Map domains to IPv4 addresses

Parameter	Description	Line 1	Line 2
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	www	www
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default	ISP_China Telecom

Parameter	Description	Line 1	Line 2
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	Default value: 300	Default value: 300
Value	Returned result of domain name resolution. For details, see **Table 2-5**.	1.1.1.1	2.2.2.2
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1	1

Parameter	Description	Line 1	Line 2
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	-	-

5. Click **OK**.

2.5.3 Configuring Region Lines

Background

Usually, a DNS server returns the same IP address to all visitors, irrespective of where they come from. This may cause high latency in cross-region access.

If you configure region lines when you create record sets, the DNS server returns different IP addresses to visitors based on their locations.

NOTE

Region lines can be used only in public zones. You cannot specify region lines for private zones or PTR records.

For example, you have built a website using domain name example.com and hosted the website on two servers, one in Chinese mainland and the other in a region outside the Chinese mainland. You need to configure three lines: **Default**, **Region** > **Chinese Mainland**, and **Region** > **Abroad**.

Region Lines

Region lines are categorized by geographic areas, as shown in **Table 2-22**.

Table 2-22 Region lines

Level 1	Level 2	Level 3
Chinese Mainland	All regions	Default
	North China	Beijing, Tianjin, Hebei, Shanxi, and Inner Mongolia
	Northeast China	Liaoning, Jilin, and Heilongjiang
	Northwest China	Shaanxi, Gansu, Qinghai, Ningxia, and Xinjiang
	Central China	Henan, Hubei, and Hunan
	East China	Shanghai, Jiangsu, Zhejiang, Anhui, Fujian, Jiangxi, and Shandong
	South China	Guangdong, Hainan, and Guangxi
	Southwest China	Chongqing, Sichuan, Guizhou, Yunnan, and Xizang
Abroad	All regions	Default

Suppose you have configured the following resolution lines for example.com:

- **Default**: 1.1.1.1
- **Chinese Mainland**: 2.2.2.2
- **Asia-Pacific_Hong Kong (China)**: 3.3.3.3

When a visitor in Shanghai requests the domain name example.com, IP address 2.2.2.2 is returned. When a visitor in Hong Kong requests this domain name, IP address 3.3.3.3 is returned. When a visitor in New Zealand requests this domain name, IP address 1.1.1.1 is returned.

Procedure

Configure region lines for your public domain names hosted on the DNS service.

The following describes how to configure a **Default** line to map the domain name to 1.1.1.1 and an **Asia-Pacific _Hong Kong (China)** line to map the domain name to 3.3.3.3.

1. Go to the **Public Zones** page.
2. On the **Public Zones** page, click the domain name (**example.com**) of the public zone.
3. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
4. Add two A record sets for example.com. Configure the parameters based on **Table 2-23**.

Table 2-23 Parameters for adding an A record set

Parameter	Description	Line 1	Line 2
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**. An A record set is selected here.	A – Map domains to IPv4 addresses	A – Map domains to IPv4 addresses
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • ***: The domain name is *.example.com. It covers all subdomains of example.com.	www	www

Parameter	Description	Line 1	Line 2
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Default	Select **Region** and **Asia Pacific** > **Hong Kong (China)**.
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	Default value: 300	Default value: 300
Value	Returned result of domain name resolution. For details, see **Table 2-5**.	1.1.1.1	3.3.3.3
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1	1

Parameter	Description	Line 1	Line 2
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	-	-

5. Click **OK**.

2.5.4 Configuring Custom Lines

Scenarios

Public DNS resolution provides you with more than 300 carrier and region lines. You can also configure custom resolution lines based on specific IP address ranges. Usually, a DNS server returns the same IP address to all visitors, irrespective of where they come from. With custom lines, the DNS server returns a specific IP address based on the IP addresses of visitors.

NOTE

- If the local DNS server of the broadband service provider used by the visitor does not support the Extension Mechanisms for DNS (EDNS), the authoritative DNS server checks whether the public IP address of the local DNS server matches the configured IP address range of the custom line.
- If the local DNS server of the broadband service provider used by the visitor supports EDNS, the authoritative DNS server checks whether the visitor's public IP address encapsulated in the EDNS matches the configured IP address range of the custom line.
- If IP address scheduling through ISP lines or region lines is inaccurate, you can configure custom lines to address this issue.

You can configure custom resolution lines to obtain different resolution results based on source IP addresses of visitors.

If your website (example.com) is providing services both for external and internal users, you can configure different resolution lines so that the DNS server can return the external server address (1.1.1.1) to external users and internal server address (2.2.2.2) to internal users.

Add Custom Resolution Lines

1. Go to the **Custom Lines** page.
2. Click **Add Custom Line**.
3. Configure the parameters based on **Table 2-24**.

   Table 2-24 Parameters for adding a custom resolution line

Parameter	Description	Value 1	Value 2
Line Name	Custom line name	Line 1	Line 2
IP Address Range	Source IP address range Enter a range of 1 to 50 IP addresses and separate the start and end IP addresses with a hyphen (-).	1.0.0.1-1.0.0.2	1.0.0.3-1.0.0.4

4. Click **OK**.

Add Record Sets with Custom Lines

For example, add record sets for example.com with Line 1 (to IP address 1.1.1.1) and Line 2 (to IP address 2.2.2.2).

1. Go to the **Public Zones** page.
2. On the **Public Zones** page, click the domain name (**example.com**) of the public zone.
3. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
4. Add two A record sets for example.com. Configure the parameters based on **Table 2-25**.

Table 2-25 Parameters for adding an A record set

Parameter	Description	Line 1	Line 2
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 2-5**. An A record set is selected here.	A – Map domains to IPv4 addresses	A – Map domains to IPv4 addresses
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	www	www

Parameter	Description	Line 1	Line 2
Line	Resolution line. The DNS server will return the IP address of the specified line, depending on where end users come from. The default value is **Default**. • **Default**: returns the default resolution result irrespective of where the visitors come from. • **ISP**: returns the resolution result based on end users' carrier networks. For details, see **Configuring ISP Lines**. • **Region**: returns the resolution result based on end users' geographical locations. For details, see **Configuring Region Lines**.	Resolution Lines_Line1	Resolution Lines_Line2
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	Default value: 300	Default value: 300
Value	Returned result of domain name resolution. For details, see **Table 2-5**.	1.1.1.1	2.2.2.2
Weight	Weight for the record set. Default value: **1** Value range: **0** to **1000** If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set. For details, see **Configuring Weighted Routing**.	1	1

Parameter	Description	Line 1	Line 2
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@ Tag value. The value: • Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_key1 example_value1	example_key1 example_value1
Description	Supplementary information about the record set. Can contain a maximum of 255 characters.	-	-

5. Click **OK**.

2.5.5 Configuring Weighted Routing

Scenarios

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

The DNS service allows you to set weights to record sets to route the requests to different servers based on the specified weights. If the weight of a record set is set to 0, no result will be returned.

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

For example, you have a website deployed on three servers. The domain name of your website is example.com, and the IP addresses of the three servers are 198.xx.xx.100, 198.xx.xx.101, and 198.xx.xx.102.

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

  For details, see **How Is a Domain Name Resolved When a Record Set Has Multiple Values?**
- You add three A record sets, with each having an IP address as its value.

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

Weighted routing can better distribute requests and balance server load. You can perform the operations provided in this section to set the weights for record sets of public zones.

Constraints

Explicit and implicit URL record sets do not support weight configuration.

Preparations

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

Table 2-26 Weight setting plans

Plan	Domain Name	Record Set Type	Line	Value	Weight	Description
1	example.com	A	Default	198.xx.xx.100	1	Requests are evenly distributed to three servers (the proportion of requests is 1:1:1).
				198.xx.xx.101	1	
				198.xx.xx.102	1	

Plan	Domain Name	Record Set Type	Line	Value	Weight	Description
2	example.com	A	Default	198.xx.xx.100	2	Requests are distributed to three servers in a proportion of 2:3:1. For example, if there are six requests, two are routed to the server whose IP address is 198.xx.xx.100, three are routed to the server whose IP address is 198.xx.xx.101, and one is routed to the server whose IP address is 198.xx.xx.102.
				198.xx.xx.101	3	
				198.xx.xx.102	1	

Prerequisites

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

Procedure

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

1. Go to the **Public Zones** page.
2. On the **Public Zones** page, click the domain name (**example.com**) of the public zone.
3. Click **Add Record Set**.
4. Configure the parameters as follows:
   - **Type**: Retain the default setting **A – Map domains to IPv4 addresses**.
   - **Name**: Leave this parameter blank. This is a record set for domain name example.com.
   - **Line**: Select **Default**.
   - **Value**: Set it to **198.xx.xx.100**, the IP address of the first website server.
   - **Advanced Settings** > **Weight**: Set it to **1**.
5. Click **OK**.
6. Repeat **3** to **5** to add the second and third record sets.

   Set the record set value to 198.xx.xx.101 and 198.xx.xx.102, respectively.

   Requests will be evenly distributed to the three servers.

3 Private Domain Name Resolution

3.1 Overview

What Is Private Domain Resolution?

A private domain name is a domain name that takes effect in a VPC. DNS allows you to map private domain names to private IP addresses and resolves domain names for other cloud services within VPCs.

Private domain names have the following features:

- You can create any private domain names without registering them.
- One private domain name can be associated with multiple VPCs and is valid only in VPCs. There is no limit on the number of associated VPCs.

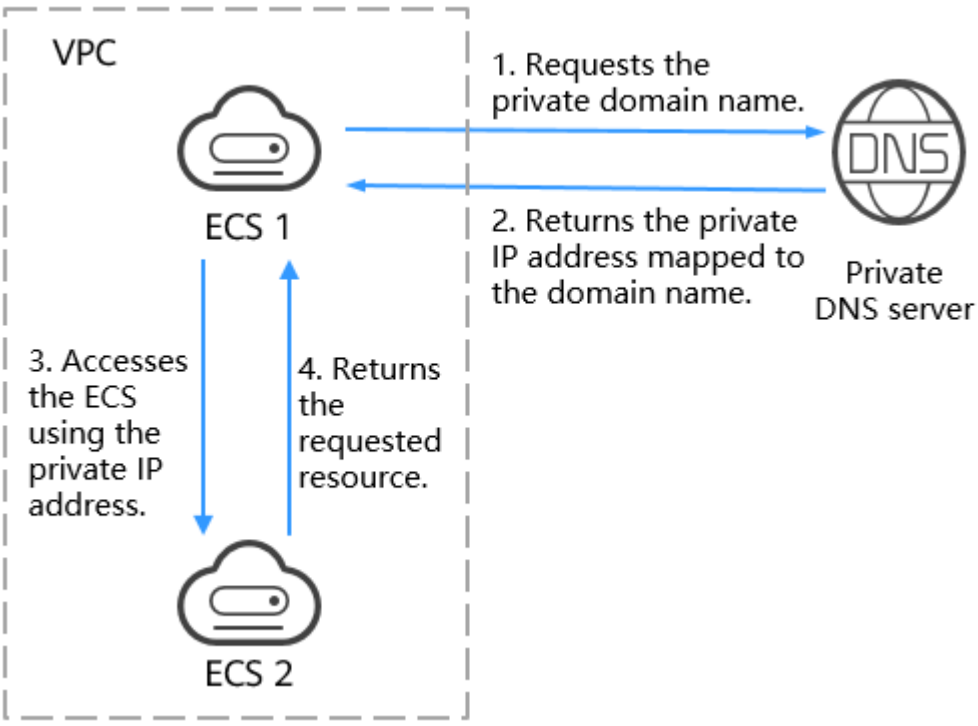
To resolve private domain names, you need to create a private zone and associate it with VPCs as needed.

Private DNS resolution translates domain names like ecs.com and their subdomains used within one or more VPCs to private IP addresses (such as 192.168.1.1). With private domain name resolution, ECSs within a VPC can communicate with each other using private zones. These ECSs can also access cloud services, such as Object Storage Service (OBS) and Simple Message Notification (SMN), over a private network.

Resolution Process

Figure 3-1 shows the resolution process.

Figure 3-1 Resolution process



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.

Scenarios

Private domain name resolution is applicable to the scenarios below.

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. This helps you manage ECSs more easily.

For example, if you have deployed 20 ECSs in an AZ, 10 used for website A and 10 for website B, you can plan their host names and private zones 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 configuring the preceding private zones, you will be able to quickly determine the locations and usages of ECSs during routine management and maintenance.

For detailed operations, see **Routing Traffic Within VPCs**.

ECS Switchover Without Service Interruption

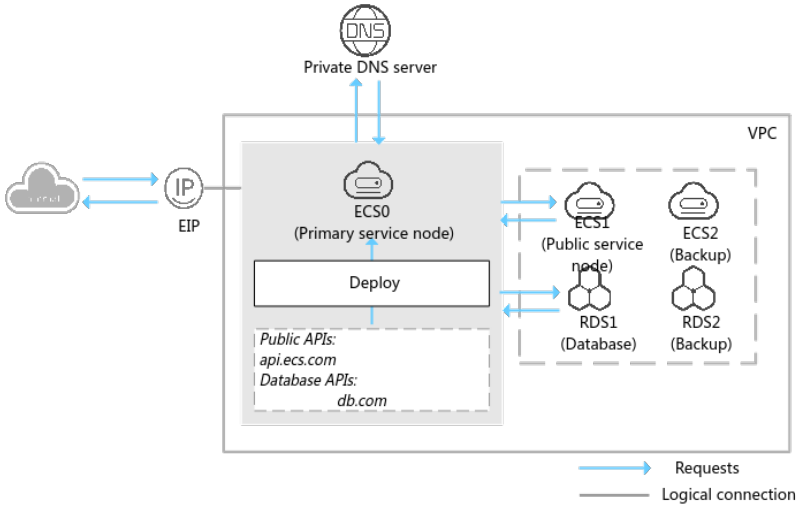
As Internet users are surging, a website application deployed only on one server may corrupt upon spiking concurrent requests. The common practice is to spread service load to multiple servers.

Multiple ECSs are deployed in the same VPC and communicate with each other using private IP addresses. The private IP addresses are coded into the internal APIs called among the ECSs. If one ECS is replaced in the system, the private IP address changes accordingly. In this case, you also need to change that IP address in the APIs and re-publish the website. This makes system maintenance inconvenient.

If you create a private zone for each ECS and configure record sets to map their private zones to the private IP addresses, the ECSs will be able to communicate over private zones. When you replace one of the ECSs, you only need to change the IP address in record sets, instead of modifying the code.

Figure 3-2 shows a typical application scenario of private zones.

Figure 3-2 Configuring private zones for ECSs



ECS and RDS are deployed in a VPC. ECS and RDS nodes are described as follows:

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

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. Such change will interrupt services, and you must publish the website again.

Now assume that you have configured private zones for the ECSs and have written these zones in the code. After ECS1 becomes faulty, you only need to change the DNS records to redirect services to ECS2, without interrupting services or re-publish the website.

For more details, see **Configuring a Private Domain Name for an ECS**.

Accessing Cloud Resources

Configure private zones 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 DNS servers are configured for the VPC subnet where the ECS is running, requests to access cloud services will be routed over the Internet.

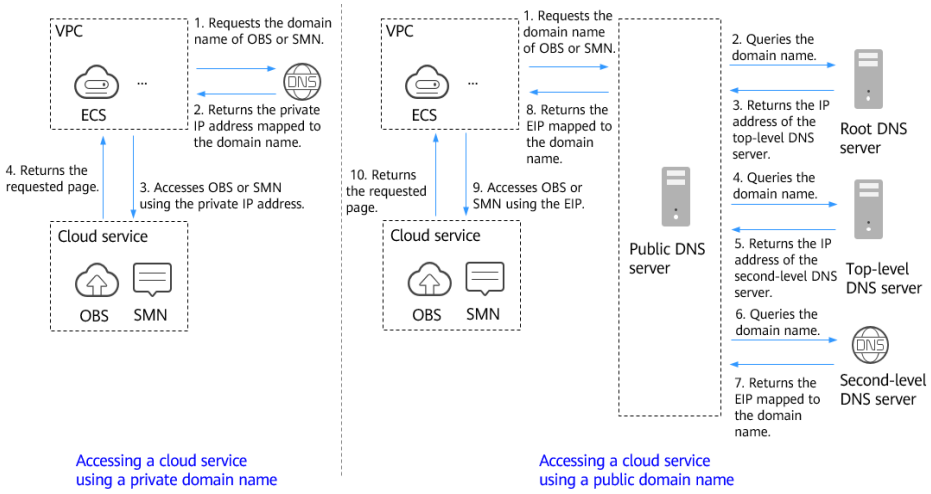
  Figure 3-3 shows the process for resolving a domain name when an ECS accesses Huawei cloud services such as OBS and SMN.

  The request directed to the Internet has long access latency and poor 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 Huawei cloud services, the private DNS server returns their private IP addresses, instead of routing requests over the Internet. This reduces network latency and improves access speed. Steps 1 to 4 on the left of **Figure 3-3** shows the process.

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

Figure 3-3 Accessing cloud services



3.2 Private Zones

3.2.1 Creating a Private Zone

Scenarios

To start hosting your private domain name in Huawei Cloud DNS, you first need to create a private zone to map the 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 a private domain name (example.com) for the ECS.

Procedure

1. Go to the **Private Zones** page.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click **Create Private Zone**.
4. Configure the parameters.
   Table 3-1 describes the parameters.

   Table 3-1 Parameters for creating a private zone

Parameter	Description	Example
Domain Name	Domain name you have planned for the ECS. You can enter a top-level domain that complies with the domain naming rules.	example.com
Recursive resolution proxy for subdomains	If you select this option, when you query subdomains that are not configured in the zone namespace, DNS will forward the DNS queries to the Internet for recursive resolution and use the result from authoritative DNS servers.	-
VPC	VPC to be associated with the private zone. **NOTE** This VPC you choose must be the VPC where your servers (such as ECSs) are. 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

Parameter	Description	Example
Enterprise Project	Enterprise project associated with the private zone. You can manage private zones by enterprise project. This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**. When configuring this parameter, note the following: • If you do not manage zones by enterprise project, select the **default** enterprise project. • If you manage zones by enterprise project, select an existing enterprise project. Before you configure this parameter, **create an enterprise project**.	default
Tag	Optional. Identifier of the zone. Each tag contains a key and a value. You can add up to 20 tags to a zone. For details about tag key and value requirements, see **Table 3-2**.	example_key1 example_value1
Description	(Optional) Supplementary information about the zone. The description can contain a maximum of 255 characters.	This is a zone example.

Table 3-2 Tag key and value requirements

Parameter	Requirements	Example
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@	example_key1

Parameter	Requirements	Example
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_value1

5. Click **OK**.
6. Switch back to the **Private Zones** page.

   You can view the created private zone on the **Private Zones** page.
7. On the **Private Zones** page, locate the private zone you created and click the domain name.

   On the **Record Sets** tab, click **Add Record Set**.

   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 **Adding Record Sets for a Private Zone**.
- Modify or delete the private zone, or view its details. For details, see **Managing Private Zones**.

3.2.2 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, enable or disable the recursive resolution proxy for subdomains, and update the description of a private zone.

NOTE

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

1. Go to the **Private Zones** page.

2. Click  in the upper left corner and select the desired region and project.
3. Locate the private zone you want to modify and choose **More** > **Modify** in the **Operation** column.
4. Modify the private zone.
5. 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. Go to the **Private Zones** page.
2. Locate the private zone you want to delete and choose **More** > **Delete** in the **Operation** column.

   The **Delete Private Zone** dialog box is displayed.
3. In the displayed dialog box, confirm the private zone to be deleted.

   Enter **DELETE** and click **OK**.

Deleting Private Zones

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

NOTICE

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

1. Go to the **Private Zones** page.
2. Select the private zones you want to delete and click **Delete**.
3. In the displayed dialog box, confirm the private zones to be deleted.

   Enter **DELETE** and click **OK**.

Viewing Details About a Private Zone

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

1. Go to the **Private Zones** page.
2. In the private zone list, view the domain name, status, associated VPCs, number of record sets, TTL, tags, time when the zone was created and when it was modified recently.

Disabling or Enabling a Private Zone

Disable a private zone to stop all record sets in the private zone. When you want to restore the resolution of the domain name, enable the private zone.

1. Go to the **Private Zones** page.
2. Select the private zone you want to disable or enable and click **Disable** or **Enable** in the **Operation** column.

   The **Disable Private Zone** or **Enable Private Zone** dialog box is displayed.
3. Click **OK**.

3.2.3 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 you choose must be the VPC where your servers (such as ECSs) are. Otherwise, the domain name cannot be resolved.

Procedure

1. Go to the **Private Zones** page.
2. Click in the upper left corner and select the desired region and project.
3. Locate the private zone with which you want to associate the VPC and click **Associate VPC** in the **Operation** column.
4. 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.
5. Click **OK**.

   The VPC is displayed in the **Associated VPCs** column.

3.2.4 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.

Constraints

If only one VPC is associated with a private zone, you cannot disassociate the VPC from the private zone. To prevent the private zone from taking effect in the VPC, you can directly delete the private zone.

Procedure

1. Go to the **Private Zones** page.
2. Click in the upper left corner and select the desired region and project.
3. Locate the private zone from which a VPC is to be disassociated, select the VPC to be disassociated in the **Associated VPCs** column, and click on the right of the VPC.
4. In the **Disassociate VPC** dialog box, click **OK**.

3.3 DNS Rules

3.3.1 Record Set Types and Configuration Rules

Record Set Types and Configuration Rules

Private zones support the following record set types: A, CNAME, MX, AAAA, TXT, SRV, NS, SOA, and PTR. **Table 3-3** lists the record set types and configuration rules.

Table 3-3 Record set types and configuration rules

Record Set Type	Description	Rule	Example
A	Maps a domain name to specified IPv4 addresses.	Enter the IPv4 addresses mapped to the domain name. You can enter up to 50 different IP addresses, each on a separate line.	192.168.xx.2 192.168.xx.3
CNAME	Maps one domain name to another or multiple domain names to one.	Enter the domain name to which you want to map your domain names. You can enter only one domain name.	www.example.com

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

Record Set Type	Description	Rule	Example
TXT	Identifies a domain name. Scenarios: • Record DKIM public keys to prevent email fraud. • Record the identity of domain name owners to facilitate domain name retrieval.	Enter text content as required. 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 4,096 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" • SPF TXT record: "v=spf1 a mx -all" Only IP addresses in the A and MX record sets are authorized to send emails using this domain name.

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

Record Set Type	Description	Rule	Example
NS	Delegates subdomains to other name servers. For private zones, an NS 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.	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.	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 a domain name.	Private domain name mapped to the private IP address. You can specify only one domain name. **PTR record sets can only be added to private domain names whose top-level domain is in-addr.arpa.**	www.example.com

Wildcard Resolution Rules

DNS allows you to set the record set name to a wildcard (*) (for example, *.example.com). In this way, access requests to all subdomains will be resolved to the same record set.

If you configure a wildcard record set for a domain name and add multiple record sets of the same record type for a specific subdomain, the priority rule for domain name resolution is as follows: **exact record set query > wildcard record set query.**

Take example.com as an example.

1. Configure a wildcard record set and a record set with its name specified.

Subdomain	Record Set Type	Value
*.example.com	A	192.168.xx.2

2. Configure record sets with the same type for subdomain **www.example.com**.

Subdomain	Record Set Type	Value
www.example.com	**A**	**192.168.xx.3**
*.example.com	A	192.168.xx.2

When a user accesses the domain name **www.example.com**, **192.168.xx.3** is returned.

Rule: If both wildcard and exact domain name queries are matched, the exact domain name query result prevails.

TTL Setting Rules

Time-To-Live (TTL) specifies how long the local DNS server (Local DNS) should cache a record. It is measured in seconds. Common TTL values include 300 seconds (5 minutes), 3,600 seconds (1 hour), and 86,400 seconds (24 hours). The default TTL value for Huawei Cloud DNS is 300 seconds.

When receiving a query for a domain name, the local DNS server queries the private DNS server and then caches the obtained record to the local server. The cache period is defined by the TTL value specified in the record.

- During this TTL period, if the local DNS server receives requests for this domain name again, it returns the cached record without requesting the record from the private DNS server.
- When the TTL expires, the local DNS server clears the cached records. If the local DNS server receives a query for the domain name, it queries the private DNS server for the domain to get a fresh record and caches the record.

Table 3-4 Application scenarios of TTL

TTL Setting	Scenario	Description
Increase the TTL value.	Reducing network traffic	A larger TTL value allows DNS records to be cached on the client or server for a longer period. This reduces queries to the DNS server and network load.
	Faster response	In IP packets, a larger TTL value allows packets to survive longer on the network. This reduces the number of requests and prevents network congestion.

TTL Setting	Scenario	Description
	Stable network	In a stable network with low packet loss, a large TTL value can improve data transmission efficiency by avoiding the need for retransmissions.
Decrease the TTL value.	Quick update	• For frequently updated content such as that from news websites or social media, a small TTL ensures that users can obtain the latest information promptly and reduces the delay caused by caching. • A small TTL can quickly clear the old cache and ensure faster update of DNS records. This ensures that the clients can use the latest records sooner.
	Testing and diagnosis	In network tests, if you set a small TTL value, packets will not stay on the network for a long time. This allows you to quickly identify, trace, analyze, and troubleshoot network issues.
	Dynamic network environment	A small TTL value can minimize the impact of outdated routing data on a network where routes are frequently changing. This improves network adaptability and response speed.
	Reducing network congestion	A small TTL value can help prevent network congestion, particularly in bandwidth-constrained environments.

To set the TTL value, you need to consider both the stability and update requirements of records. Set a long TTL for stable records and a short TTL for frequently changing records. Pay attention to the following:

- **A balance between load and response**: When adjusting the TTL value, you need to balance the network load and response speed. This aims to prevent delays in updates out of a high TTL value or load increase out of a low TTL value.
- **Network environment evaluation**: You need to set an appropriate TTL value after considering both the network stability and packet loss rate.
- **Monitoring and testing**: After adjusting the TTL value, you need to monitor and test its impact to ensure the desired outcome and make further adjustments if needed.
- **Change management**: Before changing a DNS record, such as changing the server IP address, you are advised to reduce the TTL value so that DNS caches expire faster. This allows for quicker adoption of the new record. Once the change is fully propagated, you can set the TTL to its original value.

3.3.2 Rules for Handling Record Set Conflicts

Causes for Record Set Conflicts

Some record sets of the same name and line but different types cannot coexist. Otherwise, the resolution fails.

The possible causes are as follows:

- **Restrictions on CNAME record sets**: A CNAME record set cannot coexist with record sets of other types. For example, if a subdomain already has a CNAME record set configured, it cannot have other types of record sets, such as A, MX, and TXT. Otherwise, resolution may fail.
- **Resolution sequence and priority**: The DNS server resolves a domain name based on the record set type and priority. Improper configuration may cause resolution failure or conflict.
- **Multiple resolution paths**: If a domain name has multiple record sets of different types, the DNS server resolves the domain name through different paths. This results in inconsistent or conflicting resolution results.

According to the DNS standard RFC protocol, the CNAME record set has the highest priority. If CNAME and other types (such as MX) of record sets coexist, the CNAME record set hijacks MX record set in specific scenarios. As a result, the mailbox cannot send or receive emails.

For example, if the local DNS has requested and cached the CNAME record set, when the client requests the MX record set (using the mailbox to send emails), the local DNS preferentially returns the cached CNAME record set instead of requesting the MX record set from the Internet. In this case, the MX record set of the email server cannot be obtained. As a result, the mailbox fails to send emails.

Record Set Conflict Rules

If message "This record set is in conflict with an existing one" is displayed, the record set you are trying to add conflicts with or is the same as an existing record set.

Table 3-5 lists the rules.

Table 3-5 Conflicts between private zone record sets

Record Set Type	CNAME	A	AAAA	MX	TXT	PTR	SRV
CNAME	Duplicate	**Conflict**	**Conflict**	**Conflict**	**Conflict**	**Conflict**	**Conflict**
A	**Conflict**	Duplicate	No limit	No limit	No limit	No limit	No limit
AAAA	**Conflict**	No limit	Duplicate	No limit	No limit	No limit	No limit

MX	**Conflict**	No limit	No limit	Duplicate	No limit	No limit	No limit
TXT	**Conflict**	No limit	No limit	No limit	Duplicate	No limit	No limit
PTR	**Conflict**	No limit	No limit	No limit	No limit	Duplicate	No limit
SRV	**Conflict**	No limit	No limit	No limit	No limit	No limit	Duplicate

- **Conflict**: Two types of record sets cannot coexist when the names are the same.
- **No limit**: The two types of record sets can coexist.
- **Duplicate**: The record set cannot be the same as an existing one.

Record Set Conflict Troubleshooting

If message "This record set is in conflict with an existing one" is displayed, perform either of the following operations if you still want to add a record set.

- Set a different name for the record set for a subdomain of the domain name.
- Delete the existing record set and then add the record set again.

WARNING

Deleting a record set may cause domain name resolution failures. Exercise caution when performing this operation.

3.4 Record Sets

3.4.1 Overview

What Is a Record Set?

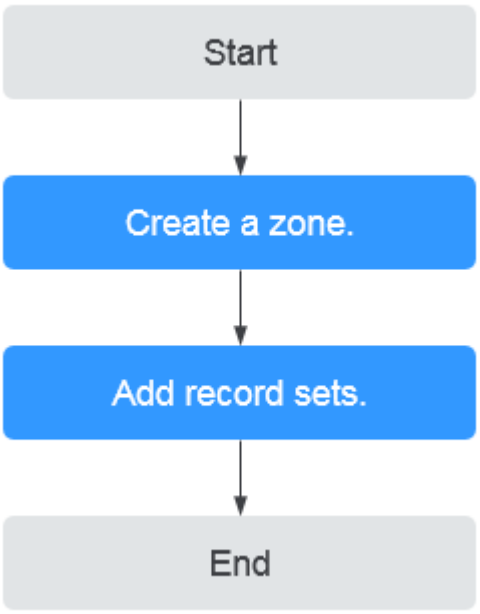
A record set translates a domain name into an IP address or other related information during DNS resolution. It defines the mapping between domain names and servers or other resources to ensure that users can find the corresponding network services when accessing domain names.

A private DNS record is used on the network of an enterprise or organization to resolve an internal domain name (for example, privatenet.example.com) to the IP address of an internal server or device. These records are stored on the internal DNS server to ensure that internal network users can quickly and securely access internal resources.

Process for Configuring a Record Set

Figure 3-4 shows the process for configuring a record set on the DNS console.

Figure 3-4 Process for configuring a record set



Related Operations

Operation	Description
Record Set Types and Configuration Rules	Learn about types, scenarios, and configuration rules of record sets supported by private zones.
Rules for Handling Record Set Conflicts	Learn about record set conflicts of private zones and how to handle the conflicts.
Adding Record Sets for a Private Zone	Configure record sets for private zones.
Configuring Recursive Resolution for Subdomains	Configure record sets for subdomains of a private zone.
Managing Record Sets	Modify a record set, delete a record set, delete records of a single domain name, and view record set details.
Disabling or Enabling Record Sets	Disable or enable record sets for a domain name. SOA and NS record sets are automatically generated and cannot be disabled.
Importing or Exporting Record Sets	Batch import or export record sets of a single zone.

3.4.2 Adding Record Sets for a Private Zone

Scenarios

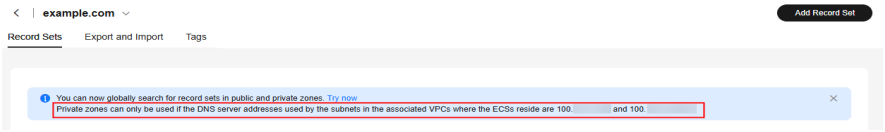
After creating a private zone for your domain name, you need to add record sets for your zone. DNS supports multiple types of record sets that apply to different service scenarios.

Record Set Type	Where to Use
A	An A record set maps domain names to IPv4 addresses of website servers. If you want to make your website accessible via a domain name, you need to add an A record set to map the domain name to the IPv4 address of your web server.
CNAME	A CNAME record set is used for scenarios like website resolution, CDN, enterprise mailbox, enterprise portal, web application firewall, object storage, and live video streaming. It maps one domain name to another domain name or multiple domain names to one domain name.
MX	An MX record set maps domain names to email servers. It is used for routing traffic to a mailbox. It records the email server's priority and domain name.
AAAA	An AAAA record set maps domain names to IPv6 addresses of website servers.
TXT	A TXT record set is used as a digital authentication certificate and for SPF (anti-spam) and domain name retrieval. It stores text-based information associated with a domain name.
SRV	An SRV record set records the services provided by servers. It is commonly used for directory management at Microsoft.
NS	An NS record set is created by default. It specifies authoritative DNS servers of domain names. **This type of record set is created by default and cannot be added manually.**
SOA	An SOA record set provides basic information about domain names and details about authoritative servers. **This type of record set is created by default and cannot be added manually.**
PTR	A PTR record set maps an IP address back to a domain name, essentially performing a reverse DNS lookup.

This section describes how to add a record set for a zone and the service scenarios and configuration rules of record sets of different types.

Constraints

- Only ECSs in the VPC associated with the private zone can access the private zone.
- 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.
  - On the **Record Sets** tab of the private zone, you can view the private DNS server addresses in the current region. The private DNS server address varies depending on the region.



  - On the VPC subnet details page, you can view the DNS server addresses used by ECSs in the **Gateway and DNS Information** area.

    Ensure that the DNS server address of the VPC subnet associated with the ECS is the same as the private DNS server address of Huawei Cloud.

Adding a Record Set

A Records

An A record maps a domain name to the private IP address of an internal server or device.

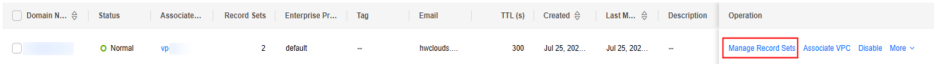
Constraints

An A record cannot coexist with a CNAME record for the same name.

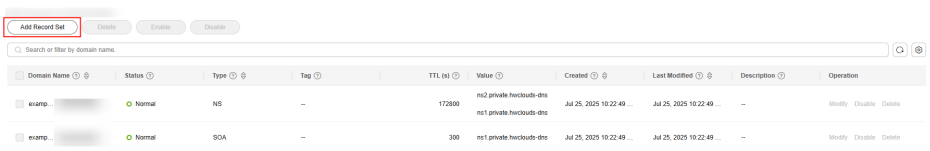
For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Private Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.



3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

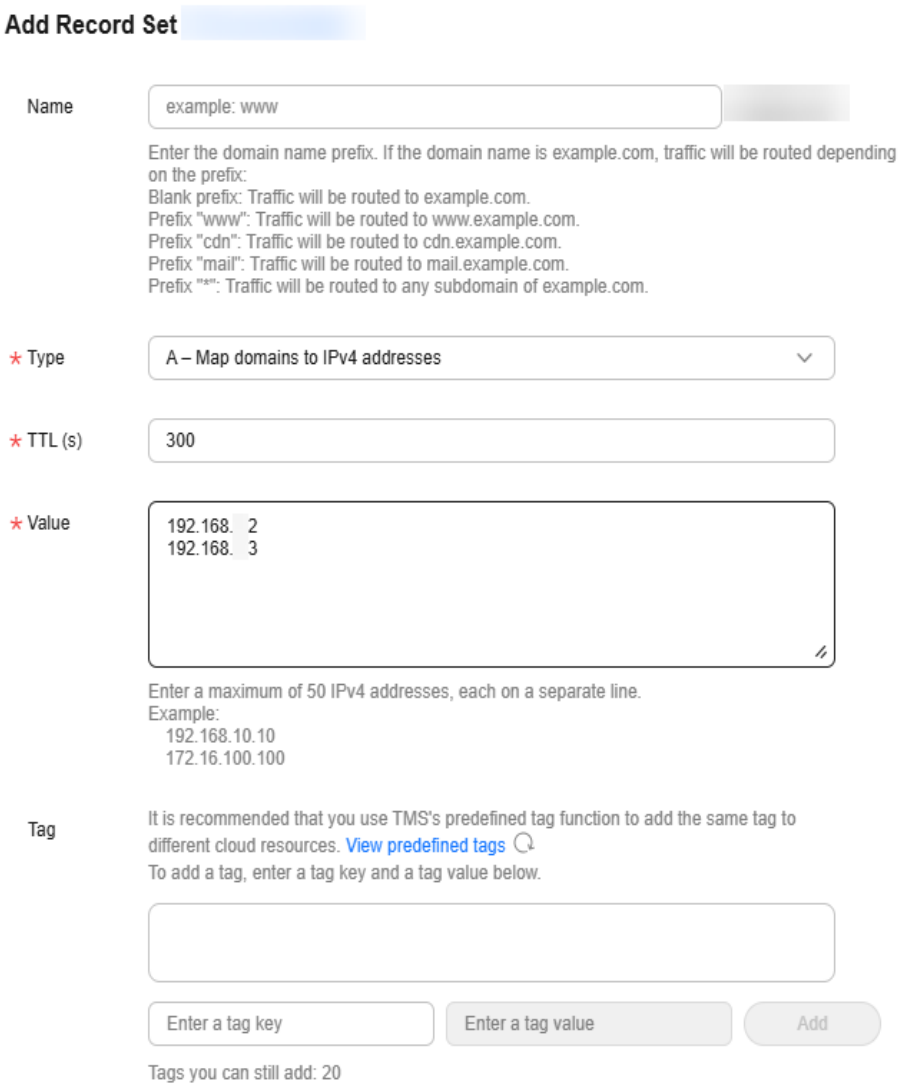


Table 3-6 Record set parameters

Parameter	Description	Example
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 3-3**.	A – Map domains to IPv4 addresses
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300
Value	Enter the IPv4 addresses mapped to the domain name. You can enter a maximum of 50 unique addresses, each on a separate line.	192.168.xx.2 192.168.xx.3

Parameter	Description	Example
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Contains a maximum of 36 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/ Tag value. The value: • Cannot be left blank. • Can contain a maximum of 43 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Record set of the private zone

5. Click **OK**.

CNAME Records

A CNAME record maps a domain name to another. CNAME records can simplify private zone management. For example, if www.internal is mapped to webserver.internal, you only need to modify the A record when the IP address of webserver.internal changes.

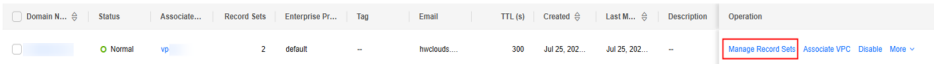
Constraints

A CNAME record cannot coexist with other types of records for the same name.

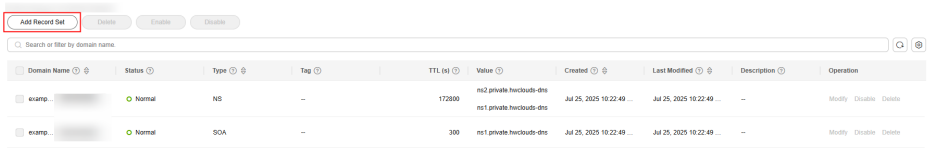
For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Private Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.



3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

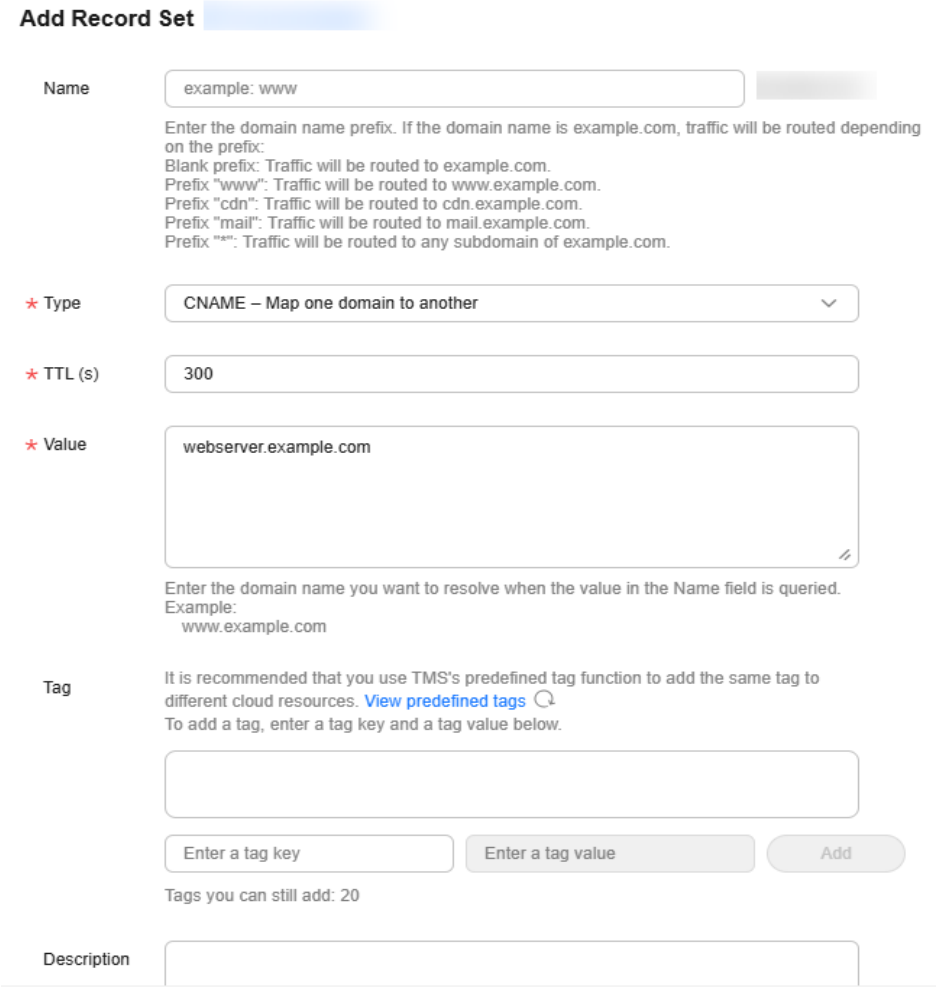


Table 3-7 Record set parameters

Parameter	Description	Example
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 3-3**.	CNAME – Map one domain to another
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300
Value	Enter the domain name that you want to point to.	webserver.example.com

Parameter	Description	Example
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Contains a maximum of 36 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/ Tag value. The value: • Cannot be left blank. • Can contain a maximum of 43 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Record set of the private zone

5. Click **OK**.

MX Records

An MX record specifies the internal mail server in private domain name resolution.

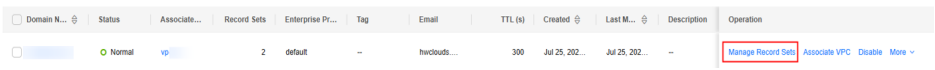
Constraints

An MX record cannot coexist with a CNAME record for the same name.

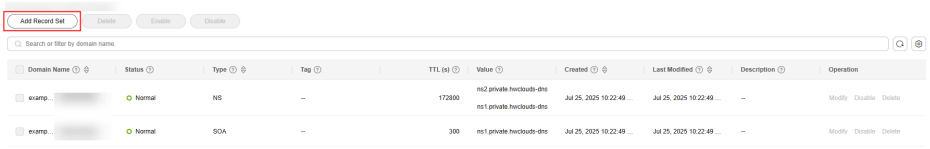
For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Private Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.



3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

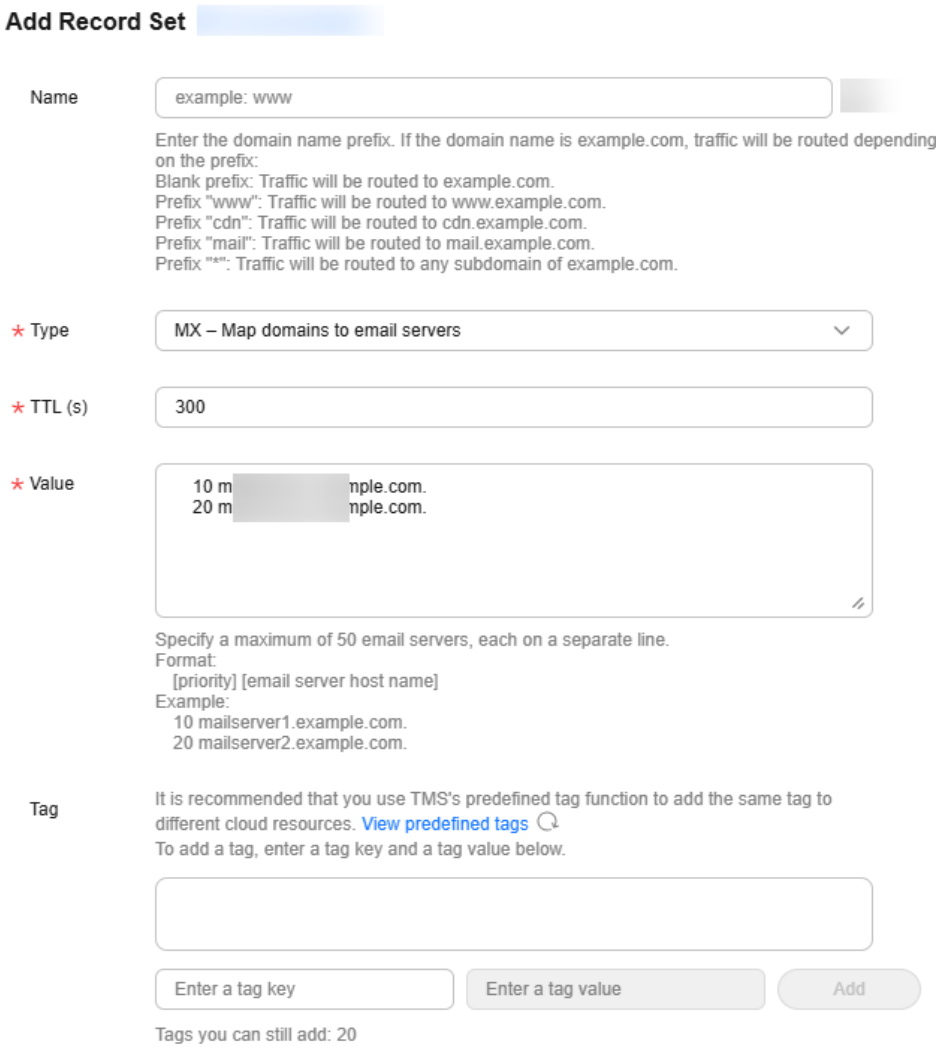


Table 3-8 Record set parameters

Parameter	Description	Example
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 3-3**.	MX – Map domains to email servers
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300

Parameter	Description	Example
Value	Enter email server addresses. You can enter a maximum of 50 unique addresses, 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.
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Contains a maximum of 36 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/ Tag value. The value: • Cannot be left blank. • Can contain a maximum of 43 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Record set of the private zone

5. Click **OK**.

AAAA Records

If the private network supports IPv6 addresses, you can add an AAAA record to map the domain name to an IPv6 address.

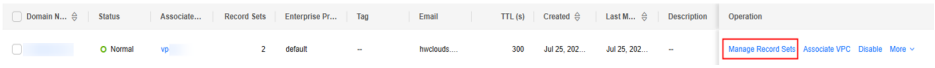
Constraints

An AAAA record cannot coexist with a CNAME record for the same name.

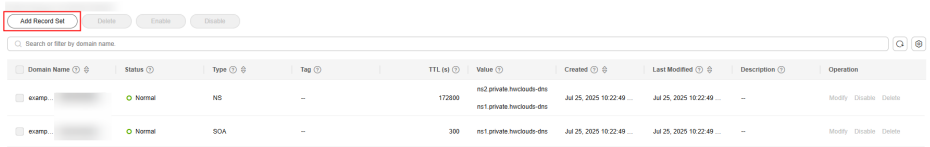
For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Private Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.



3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

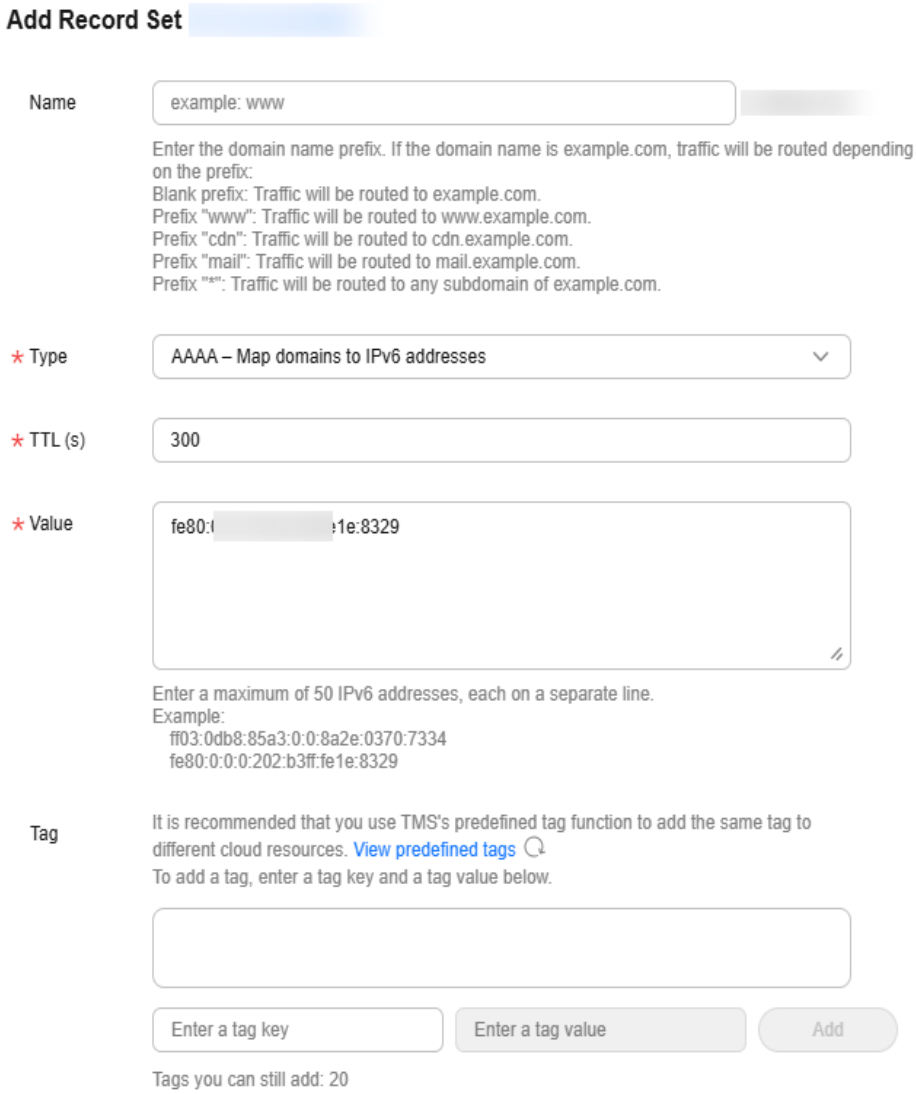


Table 3-9 Record set parameters

Parameter	Description	Example
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 3-3**.	AAAA – Map domain names to IPv6 addresses
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300
Value	Enter IPv6 addresses mapped to the domain name. You can enter up to 50 unique addresses, each on a separate line.	ff03:0db8:85a3:0:0:8a2e:0370:7334

Parameter	Description	Example
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Contains a maximum of 36 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/ Tag value. The value: • Cannot be left blank. • Can contain a maximum of 43 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Record set of the private zone

5. Click **OK**.

TXT Records

A TXT record stores Sender Policy Framework (SPF) records to prevent spam.

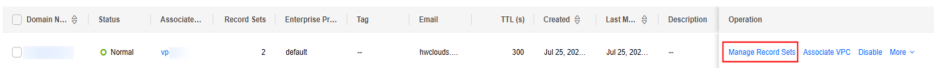
Constraints

A TXT record cannot coexist with a CNAME record for the same name.

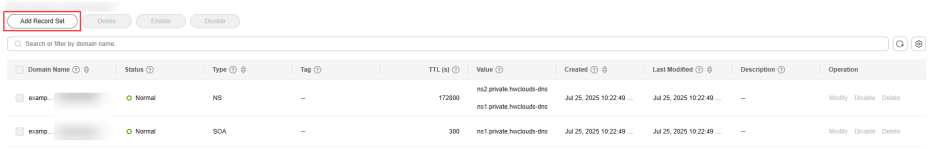
For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Private Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.



3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

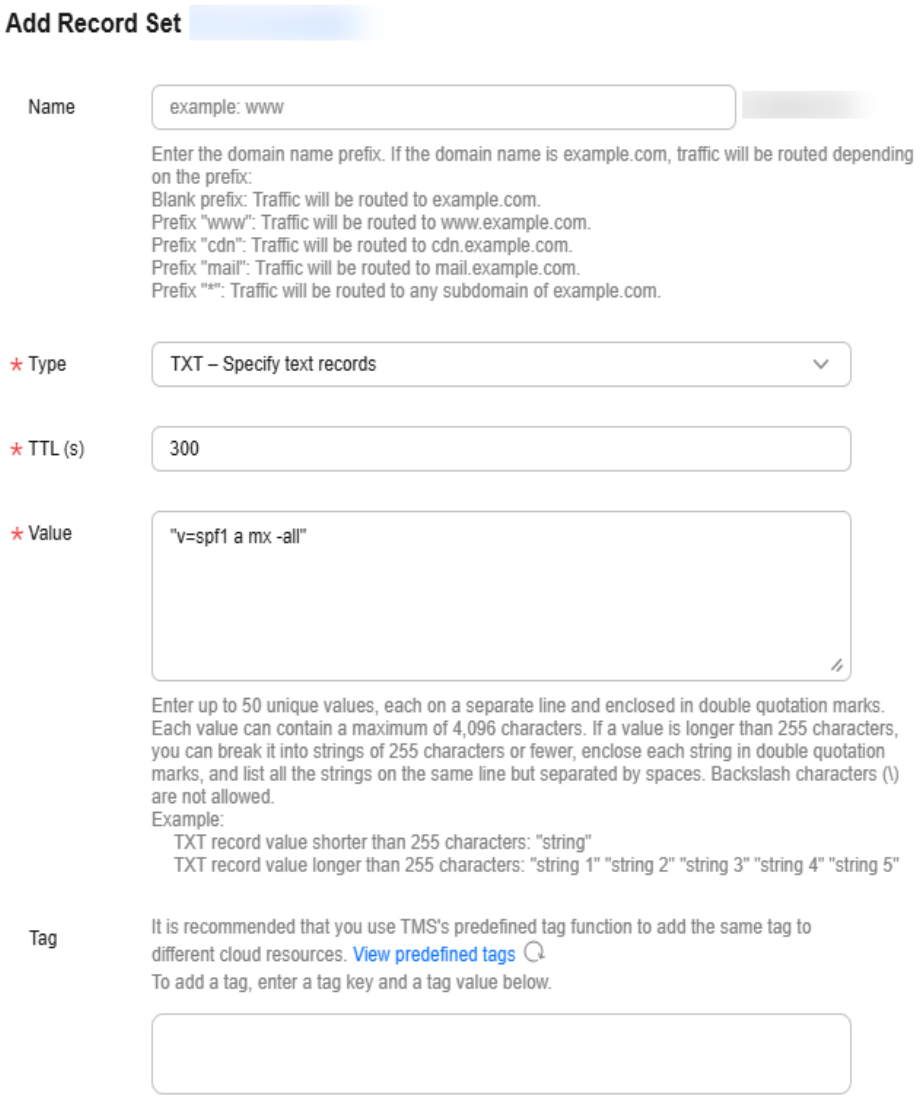


Table 3-10 Record set parameters

Parameter	Description	Example
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 3-3**.	TXT – Specify text records
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300

Parameter	Description	Example
Value	Enter text content as required. 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 4,096 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" • SPF TXT record: "v=spf1 a mx -all" Only IP addresses in the A and MX record sets are authorized to send emails using this domain name.
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Contains a maximum of 36 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/ Tag value. The value: • Cannot be left blank. • Can contain a maximum of 43 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1 example_value1

Parameter	Description	Example
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Record set of the private zone

5. Click **OK**.

SRV Records

An SRV record specifies the servers that provide specific services.

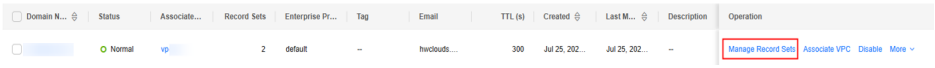
Constraints

An SRV record cannot coexist with a CNAME record for the same name.

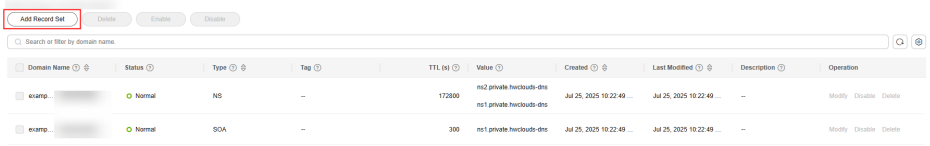
For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Private Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.



3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

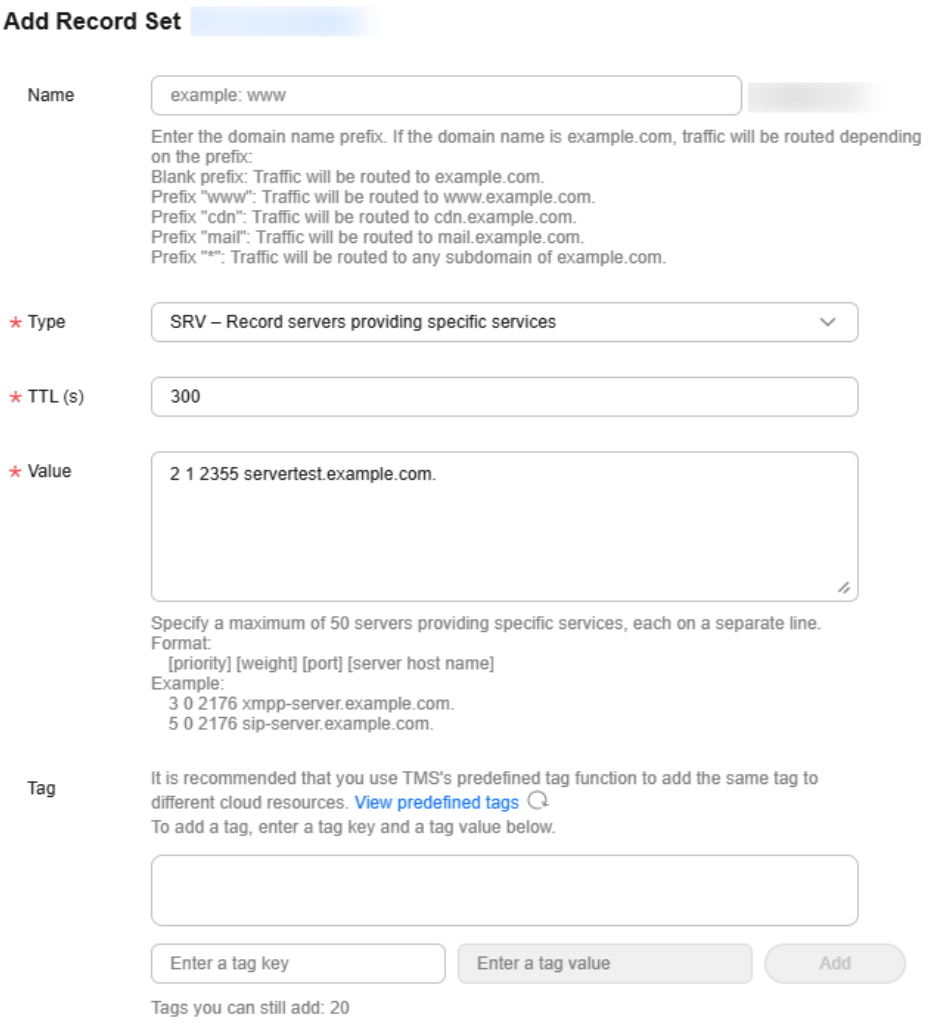


Table 3-11 Record set parameters

Parameter	Description	Example
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 3-3**.	SRV – Record servers providing specific services
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300

Parameter	Description	Example
Value	Enter the specific server addresses. You can enter a maximum of 50 unique addresses, each on a separate line. The value format is *[priority] [weight] [port] [server host name]*. Configuration rules: • The priority, weight, and port number range from 0 to 65535. • A smaller value indicates a higher priority. • A larger value indicates a larger weight. • The host name is the domain name of the target server. Ensure that the domain names can be resolved. **NOTE** If the record set values have the same priority, requests to the domain name will be routed based on weights.	2 1 2355 servertest.example.com
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Contains a maximum of 36 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/ Tag value. The value: • Cannot be left blank. • Can contain a maximum of 43 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1 example_value1

Parameter	Description	Example
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Record set of the private zone

5. Click **OK**.

PTR Records

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

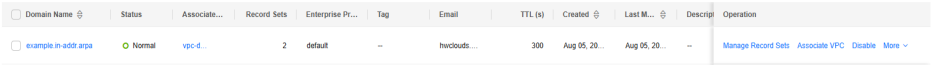
Constraints

- PTR record sets can only be added to private zones whose domain name suffix is in-addr.arpa.
- A PTR record cannot coexist with a CNAME record for the same name.

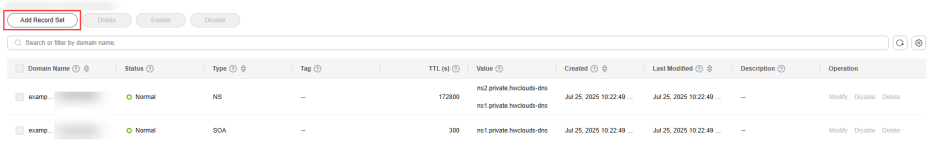
  For details about the conflict rules and handling measures, see **Rules for Handling Record Set Conflicts**.

Procedure

1. Go to the **Private Zones** page.
2. Locate the target zone and click **Manage Record Sets** in the **Operation** column.



3. Click **Add Record Set** above the record set list.



4. On the **Add Record Set** page, set record set parameters as instructed.

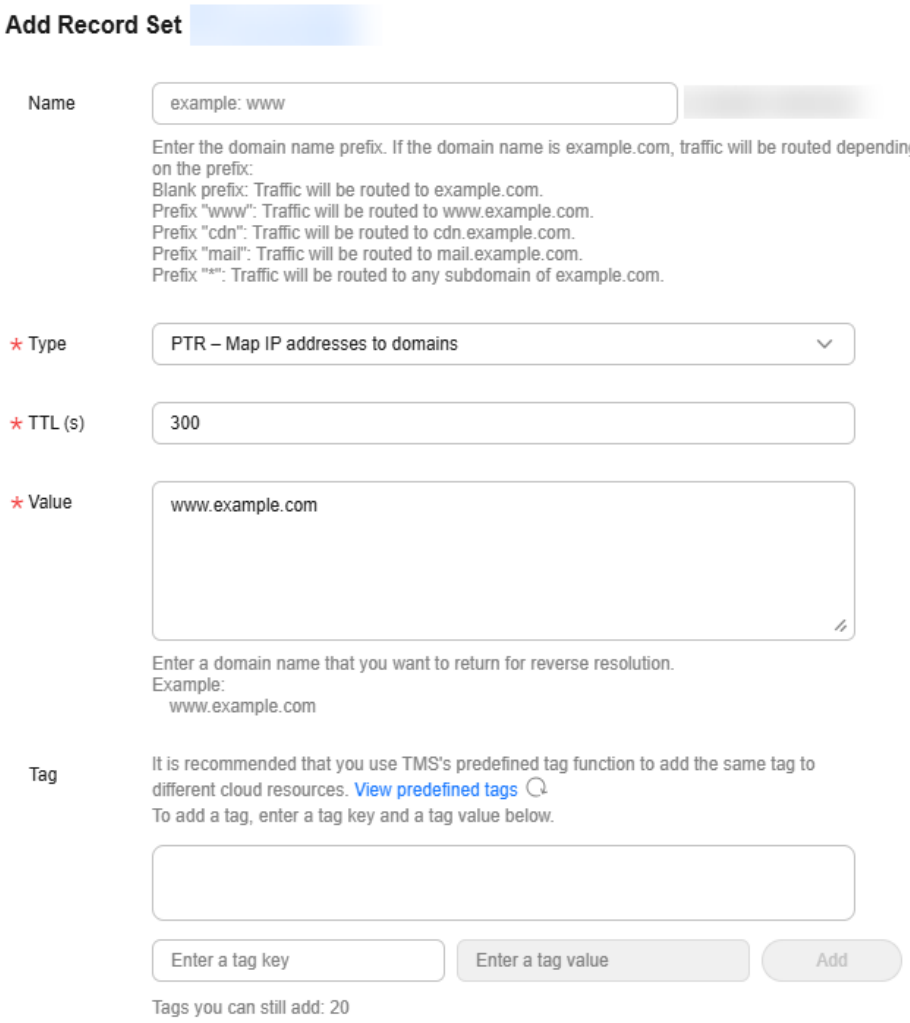


Table 3-12 Record set parameters

Parameter	Description	Example
Name	Prefix of the domain name to be resolved. This value is left empty by default. For example, if the domain name is example.com, the value of the **Name** can be as follows: • **www**: The domain name is www.example.com and usually used for a website. • Left blank: The domain name is example.com and usually used for a website. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • **abc**: The domain name is abc.example.com, a subdomain of example.com. • **mail**: The domain name is mail.example.com and usually used for email servers. • *: The domain name is *.example.com. It covers all subdomains of example.com.	Leave it blank.
Type	Record set type. Select a record set type based on service requirements. For details, see **Table 3-3**.	PTR – Map IP addresses to domains
TTL (s)	How long a local DNS server caches a DNS record. It is measured in seconds. Default value: **300** Value range: **1** to **2147483647** If your service address changes frequently, set TTL to a smaller value. Otherwise, set TTL to a larger value.	300

Parameter	Description	Example
Value	Enter the private domain name mapped to the private IP address. You can specify only one domain name. **PTR record sets can only be added to private zones whose domain name suffix is in-addr.arpa.**	www.example.com
Tag	Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags for a record set. Tag key. The key: • Cannot be left blank. • Must be unique for each resource. • Contains a maximum of 36 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/ Tag value. The value: • Cannot be left blank. • Can contain a maximum of 43 characters. • Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1 example_value1
Description	Supplementary information about the record set. The description can contain a maximum of 255 characters.	Record set of the private zone

5. Click **OK**.

3.4.3 Configuring Recursive Resolution for Subdomains

Scenarios

When creating a private zone, you can enable **Recursive resolution proxy for subdomains**. After this function is enabled, if the requested subdomain has no record set configured, the DNS service does not directly return **nxdomain** (the resolution record does not exist). Instead, the DNS service forwards the request to the Internet for resolution, starting with root servers and progressively querying

top-level domains (TLDs) and authoritative servers until the IP address of the subdomain is found.

With this function enabled, the client sends only one request and then the DNS server can handle all the steps on behalf of the client. This improves resolution efficiency and user experience.

Constraints

Private recursive DNS server does not return the resolution result based on DNS Resolver endpoint rules.

Recursive Resolution Example of a Subdomain in a Private Zone

For example.com, the following record sets have been added to the private zone:

Table 3-13 Private zone record sets

Name	Type	Value
a1	A	1.2.3.4

When a1.example.com is accessed, the DNS server returns 1.2.3.4 based on the configured private zone record set.

When www.example.com is accessed, no record sets are configured in the private zone. In this case, the authoritative DNS server resolves the domain name and returns the result.

Enabling Recursive Resolution for Subdomains

You can enable recursive subdomain resolution when creating or modifying a private zone.

- **Enabling recursive subdomain resolution when creating a private zone**

  When creating a private zone, you can select **Recursive resolution proxy for subdomains** to enable recursive subdomain resolution.

  For details about how to create a private zone, see **Creating a Private Zone**.
- **Enabling recursive subdomain resolution when modifying a private zone**

  When modifying a private zone, you can select **Recursive resolution proxy for subdomains** to enable recursive subdomain resolution.

  For details about how to modify a private zone, see **Managing Private Zones**.

3.4.4 Managing Record Sets

Scenarios

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

Modifying a Record Set

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

NOTE

- You can modify the TTL, value, and description of the NS record set.
- SOA record sets are automatically generated and cannot be modified.

1. Go to the **Private Zones** page.
2. Click  in the upper left corner and select the desired region and project.
3. In the zone list, locate the zone and click the domain name.
4. Locate the record set you want to modify and click **Modify** in the **Operation** column.
5. Modify the parameters.

   You can change the name, type, TTL, value, weight, and description.
6. Click **OK**.

Deleting a Record Set

You can delete a record set if it is no longer needed.

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

CAUTION

Deleted record sets cannot be recovered, and domain name queries will fail. Exercise caution when performing this operation.

1. Go to the **Private Zones** page.
2. Click  in the upper left corner and select the desired region and project.
3. In the zone list, locate the zone and click the domain name.
4. Locate the record set you want to delete and click **Delete** in the **Operation** column.
5. In the displayed dialog box, confirm the record set to be deleted.

   Enter **DELETE** and click **OK**.

Viewing Details About a Record Set

1. Go to the **Private Zones** page.
2. Click  in the upper left corner and select the desired region and project.
3. In the zone list, locate the zone and click the domain name.
4. Locate the record set and view the details.

3.4.5 Disabling or Enabling Record Sets

Scenarios

You can disable a zone or its record sets on the DNS console. If you disable a zone or record set, it cannot be used for resolution. You can enable the zone or record set at any time if you need it again.

This section describes how to disable or enable record sets.

Constraints

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

Disabling Record Sets

You can disable a private zone in the **Normal** state and its record sets.

1. Go to the **Private Zones** page.
2. Disable record sets.
   - **Disabling all record sets for a domain name**: In the zone list, locate the domain name and click **Disable** in the **Operation** column.
   - **Disabling a record set**: Locate the zone and click the domain name to go to the record set list. Locate the target record set, click **Disable** in the **Operation** column.
   - **Disabling multiple record sets**: Locate the zone and click the domain name to go to the record set list. Select the record sets, click **Disable** above the record set list.
3. Click **OK**.

   NOTE

   After a record set is disabled, it cannot be used for resolution, but you can view it in the record set list.

Enabling Record Sets

You can enable the record sets that have been disabled.

1. Go to the **Private Zones** page.
2. Enable record sets.
   - **Enabling all record sets for a domain name**: In the zone list, locate the domain name and click **Enable** in the **Operation** column.
   - **Enabling a record set**: Locate the zone and click the domain name to go to the record set list. Locate the target record set, click **Enable** in the **Operation** column.
   - **Enable multiple record sets**: Locate the zone and click the domain name to go to the record set list. Select the record sets, click **Enable** above the record set list.
3. Click **OK**.

3.4.6 Importing or Exporting Record Sets

Exporting Record Sets

Scenarios

If you want to transfer your domain name to another cloud service provider, you can export all the record sets configured for the domain name in batches.

The following information can be exported: domain name, type, TTL (s), value, status, description, record set ID, time when the record set was created, and time when the record set was last modified.

Procedure

1. Go to the **Private Zones** page.
2. Click  in the upper left corner and select the desired region and project.
3. In the zone list, click the name of the zone whose record sets are to be exported.
4. Click the **Export and Import** tab.
5. Click **Export Record Set** in the upper right corner of the page.

   An .xlsx file named using the domain name is exported, for example, **example.com.xlsx**.

   In the file, you can view the following information about record sets: domain name, type, TTL (s), value, status, description, record set ID, time when the record set was created, and time when the record set was last modified.

Importing Record Sets

Scenarios

If you want to transfer your domain name from another cloud server provider to the DNS service for hosting, you can import existing record sets configured for the domain name in batches.

You can import up to 500 record sets at a time.

NOTE

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

Procedure

1. Go to the **Private Zones** page.
2. Click  in the upper left corner and select the desired region and project.
3. In the zone list, click the name of the zone whose record sets are to be imported.
4. Click the **Export and Import** tab.
5. Before you import record sets, list them in the template.
   a. Click **Download template** in the note.

b. Fill in the template as required.

NOTE

If you have exported record sets from the previous service provider, you need to fill them in the template. If the format is incorrect, the import may fail.

6. In the upper right corner of the page, click **Import Record Set** and select the record set file to import.

   You can check whether record sets are imported or not.

   - **Successful Import**: The number of successfully imported record sets are displayed.
   - **Failed Import**: All failed record sets are listed. You can resolve the problems based on the causes.

NOTE

Before importing record sets again, click **Clear** in the upper right corner of the page to clear both the record sets that have been imported successfully and the record sets failed to be imported.

Common Causes and Solutions for Import Failures

Error Message	Cause	Solution
There is already an import task for this domain name. Clear the existing task and then continue the import.	The record sets that failed to be batch imported were not cleared.	Click **Clear** in the upper right corner of the **Export and Import** tab and try again.
Invalid record set type: A, AAAA, MX, CNAME, TXT, PTR, or SRV.	The types of record sets to be imported are invalid.	Modify or delete the record sets of invalid types and try again.
Invalid record set value.	The values of record sets to be imported are invalid.	Modify the record set values as needed and try again. For details, see **Record Set Types and Configuration Rules**.
Invalid record set name. The record set name must be a valid domain name.	Invalid domain name configured in the record set.	Enter **www** for the **Name** field or leave it blank. You can also enter **www.example.com.** (a domain name with a period at the end) for the **Name** field.
Invalid zone description. The description can contain a maximum of 255 characters.	The record set description exceeds 255 characters.	Change the record set description. The value can contain a maximum of 255 characters.

Error Message	Cause	Solution
Invalid TTL value.	TTL of the record sets to be imported are invalid.	Change the record set TTL. Value range: **1** to **2147483647**

4 PTR Records

4.1 Overview

What is a PTR Record?

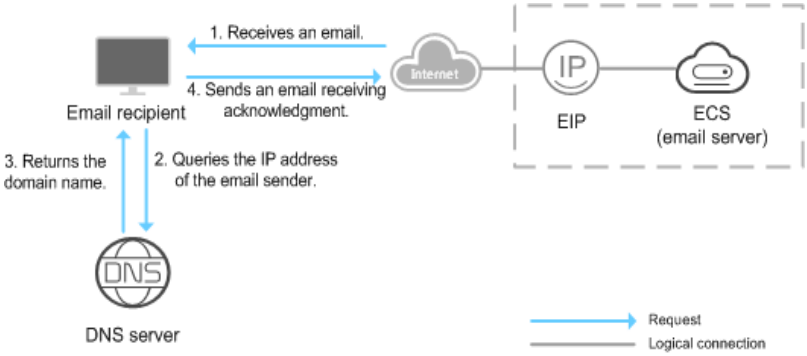
A PTR record provides the domain name associated with an IP address. It is the opposite of a regular DNS lookup. PTR records are used in many network applications. For example, email servers use reverse resolution to verify the sender's IP address to reduce spam and network fraud.

After a recipient server receives an email, it checks whether the IP address and domain name of the sender server are trustworthy and determines whether the email is spam. If the recipient server fails to obtain the domain name mapped to the sender's IP address, it concludes that the email is sent by a malicious host and rejects it. It is necessary to configure pointer records (PTR) to point the IP addresses of your email servers to domain names.

Reverse Resolution Process

In the following figure, an ECS serves as an email server, and a PTR record is configured to map the EIP of the ECS to the domain name configured for accessing the email server.

Figure 4-1 Reverse resolution



NOTE

Figure 4-1 shows only the process for reverse resolution. Information about how an email server checks the credibility of the sender's IP address and whether the domain name is available on the Internet is not provided here.

If no PTR records are configured, the recipient server will treat emails from the email server as spam or malicious and discard them. Therefore, if you want to build an email server, it is necessary to add a PTR record to map the email server IP address to your domain name.

Related Operations

Table 4-1 PTR record operations

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

4.2 Creating a PTR Record

Scenarios

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

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

NOTE

PTR records take effect only after the name servers are configured. After you create a PTR record, we will contact China Internet Network Information Center (CNNIC) or Asia Pacific Network Information Centre (APNIC) to configure the name servers and allow Huawei Cloud DNS for domain name resolution. This process takes about 1 to 7 working days. In case of urgency, submit a service ticket. We will contact CNNIC and APNIC to speed up the process.

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

Constraints

- You can only create PTR records for IP addresses with a 32-bit subnet mask.
- Only one PTR record can be created for an EIP.
- An EIP can be mapped to no more than 10 domain names.

Procedure

1. Go to the **PTR Records** page.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Create PTR Record**.
4. Configure the parameters based on **Table 4-2**.

Table 4-2 Parameters for creating a PTR record

Parameter	Description	Example
EIP	EIP of the cloud resource, for example, an ECS. You can select an EIP from the drop-down list.	xx.xx.xx.xx
Domain Name	Domain name mapped to the EIP.	example.com
TTL (s)	Cache duration of the PTR record, in seconds Default value: 300	300
Enterprise Project	Enterprise project associated with the PTR record. You can manage PTR records by enterprise project. This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**.	default
Tag	Optional. Identifier of the PTR record. Each tag contains a key and a value. You can add up to 20 tags to a PTR record. For details about tag key and value requirements, see **Table 4-3**.	example_key1 example_value1
Description	(Optional) Supplementary information about the PTR record.	The description of the PTR record

Table 4-3 Tag key and value requirements

Parameter	Requirements	Example
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@	example_key1
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and special characters _ . : / = + - @.	example_value1

5. Click **OK**.

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

   NOTE

   If a domain name needs to be mapped to multiple EIPs, you need to create a PTR record for each EIP.

6. In the DOS window of your local PC that has been connected to the Internet, check whether the PTR record takes effect.

   a. Press **Win+R** to open the **Run** dialog box, enter **cmd**, and press **Enter**.

   b. Run the following command in the DOS window:

   ```
   nslookup -qt=ptr [IP address]
   ```

4.3 Managing PTR Records

Scenarios

You can modify or delete PTR records, or view their details.

Modifying a PTR Record

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

1. Go to the **PTR Records** page.
2. Click in the upper left corner and select the desired region and project.
3. Locate the PTR record you want to modify and click **Modify** in the **Operation** column.

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

4. Change the domain name, TTL, or description as required.
5. Click **OK**.

Deleting a PTR Record

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

1. Go to the **PTR Records** page.
2. Click  in the upper left corner and select the desired region and project.
3. Locate the PTR record you want to delete and click **Delete** in the **Operation** column.
4. In the displayed dialog box, confirm the PTR record to be deleted.

   Enter **DELETE** and click **OK**.

Deleting PTR Records

Delete multiple PTR records at a time. After you delete the PTR records, the domain names mapped to your EIPs will change to the default domain names.

1. Go to the **PTR Records** page.
2. Click  in the upper left corner and select the desired region and project.
3. Select the PTR records and click **Delete**.
4. In the **Delete PTR Record** dialog box, click **OK**.

Viewing Details About a PTR Record

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

1. Go to the **PTR Records** page.
2. Click  in the upper left corner and select the desired region and project.
3. In the PTR record list, view the details.

5 Resolver

5.1 DNS Resolver Overview

What Is DNS Resolver?

DNS Resolver answers DNS queries to and from your on-premises data center after your data center is connected to the cloud over Direct Connect or VPN.

Generally, on-premises data centers can access cloud resources over a Direct Connect or VPN connection. However, for security purposes, on-premises servers are not allowed to access the DNS service on the cloud directly. If your on-premises servers need to access private domain names used within VPCs, or your cloud servers use Huawei Cloud private DNS to access an on-premises domain name, you need to set up DNS on your cloud servers for forwarding DNS queries between the cloud DNS and on-premises DNS. This increases management and maintenance costs and causes reliability risks.

With Huawei Cloud DNS Resolver, on-premises servers and cloud servers can easily communicate with each other in hybrid cloud scenarios.

Where to Use

- To enable on-premises servers to access a cloud service domain name, you need to create an inbound endpoint and configure forwarding rules on the on-premises DNS servers to forward the DNS queries for the cloud service domain name to the IP addresses specified in the inbound endpoint.

  For details, see **Managing Inbound Endpoints**.
- To allow cloud servers to access an on-premises domain name, you need to create an outbound endpoint and configure endpoint rules to specify the on-premises domain name to be accessed and the IP addresses of the on-premises DNS servers. Huawei Cloud private DNS then forwards the DNS queries for the on-premises domain name to the on-premises DNS servers based on the endpoint rules.

  For details, see **Managing Outbound Endpoints**.

5.2 Managing Inbound Endpoints

Scenarios

To enable on-premises servers to access a cloud service domain name, you need to create an inbound endpoint and configure forwarding rules on the on-premises DNS servers to forward the DNS queries for the cloud service domain name to the IP addresses specified in the inbound endpoint.

Creating an Inbound Endpoint

1. Go to the **Resolvers** page.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click **Create Endpoint**.
4. Configure the parameters based on **Table 5-1**.

Table 5-1 Parameters for creating an inbound endpoint

Parameter	Description
Endpoint Type	Type of the endpoint. There are two options: **Inbound** and **Outbound**. Select **Inbound**.
Endpoint Name	Name of the endpoint. The name can: • Contain only letters, digits, underscores (_), hyphens (-), and periods (.). • Contain 1 to 64 characters.
Region	Region where the inbound endpoint works.
VPC	The VPC over which all inbound DNS queries are forwarded to cloud DNS servers. **CAUTION** The VPC cannot be changed after an endpoint is created.
Subnet	The subnet must have available IP addresses. Only IPv4 addresses are supported.
IP Addresses	There are two options: **Automatically assign** or **Specify**. **NOTE** To improve reliability, you need to specify at least two IP addresses, with each in a different AZ. You can optionally add more IP addresses.

5. Click **Create Now**.

Viewing an Inbound Endpoint

1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.
3. On the **Inbound Endpoints** tab, locate the inbound endpoint you want to view.
4. Click the name of the inbound endpoint and view its details, such as basic configuration and IP addresses.

Modifying an Inbound Endpoint

1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.
3. On the **Inbound Endpoints** tab, locate the inbound endpoint you want to modify.
4. Click **Modify** in the **Operation** column.

   You can change the endpoint name, and add or delete IP addresses.

   NOTE

   If only two IP addresses are configured, the IP addresses cannot be deleted.

Deleting an Inbound Endpoint

1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.
3. On the **Inbound Endpoints** tab, locate the inbound endpoint you want to delete.
4. Click **Delete** in the **Operation** column.
5. Confirm the inbound endpoint and click **OK**.

5.3 Managing Outbound Endpoints

Scenarios

To allow cloud servers to access an on-premises domain name, you need to create an outbound endpoint and configure endpoint rules to specify the on-premises domain name to be accessed and the IP addresses of the on-premises DNS servers. Huawei Cloud private DNS then forwards the DNS queries for the on-premises domain name to the on-premises DNS servers based on the endpoint rules.

Creating an Outbound Endpoint

1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.

3. In the upper right corner of the page, click **Create Endpoint**.
4. Configure the parameters based on **Table 5-2**.

Table 5-2 Parameters for creating an outbound endpoint

Parameter	Description
Endpoint Type	Type of the endpoint. There are two options: **Inbound** and **Outbound**. Select **Outbound**.
Endpoint Name	Name of the endpoint. The name can: • Contain only letters, digits, underscores (_), hyphens (-), and periods (.). • Contain 1 to 64 characters.
Region	Region where the outbound endpoint works.
VPC	The VPC over which all outbound DNS requires are forwarded to the IP addresses specified in the endpoint rules. **CAUTION** The VPC cannot be changed after an endpoint is created.
Subnet	The subnet must have available IP addresses. Only IPv4 addresses are supported.
IP Address	There are two options: **Automatically assign** or **Specify**. **NOTE** To improve reliability, you need to specify at least two IP addresses, with each in a different AZ. You can optionally add more IP addresses.

5. Click **Create Now**.

NOTE

After an outbound endpoint is created, you need to configure endpoint rules. For details, see **Modifying an Outbound Endpoint** or **Adding an Endpoint Rule**.

Viewing an Outbound Endpoint

1. Go to the **Resolvers** page.
2. Click  in the upper left corner and select the desired region and project.
3. On the **Outbound Endpoints** tab, locate the outbound endpoint you want to view.
4. Click the name of the outbound endpoint and view its details, such as basic configuration, IP addresses, and endpoint rules.

Modifying an Outbound Endpoint

1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.
3. On the **Outbound Endpoints** tab, locate the outbound endpoint you want to modify.
4. Click **Modify** in the **Operation** column.

   You can change the endpoint name, add or delete IP addresses, and add or delete endpoint rules.

   NOTE

   If only two IP addresses are configured, the IP addresses cannot be deleted.

Deleting an Outbound Endpoint

1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.
3. On the **Outbound Endpoints** tab, locate the outbound endpoint you want to delete.
4. Click **Delete** in the **Operation** column.
5. Confirm the outbound endpoint and click **OK**.

5.4 Managing Endpoint Rules

Scenarios

To allow cloud servers to access an on-premises domain name, you need to create an outbound endpoint and configure endpoint rules to specify the on-premises domain name to be accessed and the IP addresses of the on-premises DNS servers. Huawei Cloud private DNS then forwards the DNS queries for the on-premises domain name to the on-premises DNS servers based on the endpoint rules.

An endpoint rule can have more than one VPC associated. After a VPC is associated with an endpoint rule, DNS queries for the on-premises domain name from the cloud servers in the VPC will be forwarded to the on-premises DNS servers.

Constraints

The domain name of the private zone you want to create and the VPCs associated with the private zone cannot conflict with the domain names configured in and VPCs associated with the DNS Resolver endpoint rules.

For example, if the example.com domain name is configured in an endpoint rule and VPC A is associated with the endpoint rule, you cannot create a private zone for example.com and associate VPC A with the private zone.

Adding an Endpoint Rule

Before adding endpoint rule, you need to create an outbound endpoint. For details, see **Creating an Outbound Endpoint**.

1. Go to the **Resolvers** page.
2. Click  in the upper left corner and select the desired region and project.
3. Click the **Endpoint Rules** tab.
4. Click **Add Endpoint Rule**.
5. Configure the parameters based on **Table 5-3**.

Table 5-3 Parameters for adding an endpoint rule

Parameter	Description
Name	Name of the endpoint rule added to an outbound endpoint.
Domain Name	Domain name used by on-premises servers.
Type	By default, **Resolver** is selected.
Outbound Endpoint	Select the outbound endpoint that you want to add this endpoint rule to.
Associate VPC	Choose whether to associate VPCs with the endpoint rule. If this option is selected, you need to select one or more VPCs.
Region	Region that the VPCs belong to. This parameter is displayed after **Associate VPC** is selected.
VPC	Select the VPCs to be associated with the endpoint rule. This parameter is displayed after **Associate VPC** is selected.
IP Addresses	IP address of a DNS server in the on-premises data center. You can add one or more IP addresses.

CAUTION

After an endpoint rule is added, the domain name, type, and outbound endpoint cannot be changed.

6. Click **OK**.

Viewing an Endpoint Rule

1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.
3. Click the **Endpoint Rules** tab to view the endpoint rule list.

   You can view the endpoint rules you created or other users shared with you.
4. Click the name of the endpoint rule to view its details, such as basic configuration, VPCs, and IP addresses.

Modifying an Endpoint Rule

1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.
3. Click the **Endpoint Rules** tab to view the endpoint rule list.
4. Locate the endpoint rule and click **Modify** in the **Operation** column.

   You can change the rule name, associate other VPCs, disassociate VPCs, and add, delete, or change IP addresses.

   NOTE

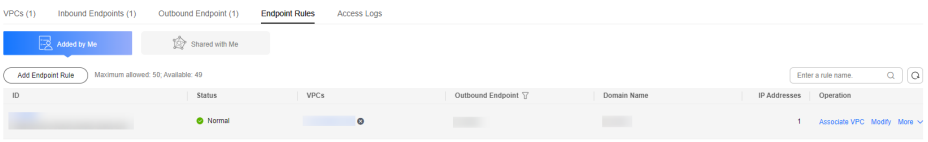
   If only one IP address is configured for the endpoint rule, the IP address cannot be deleted.

Deleting an Endpoint Rule

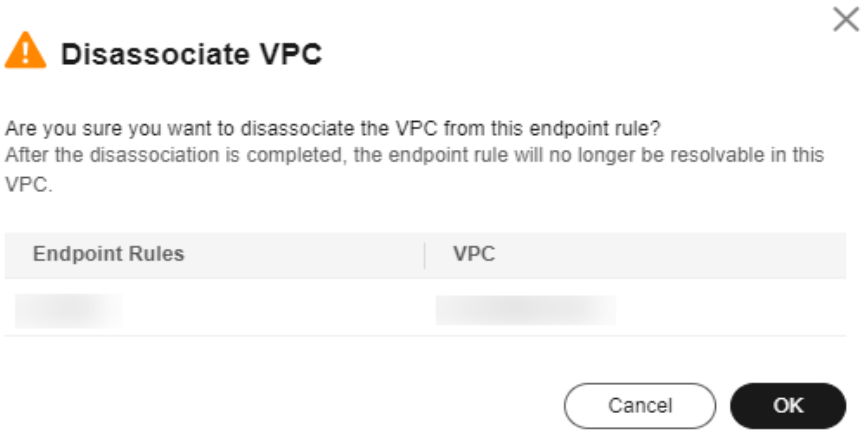
1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.
3. Click the **Endpoint Rules** tab to view the endpoint rule list.
4. Locate the endpoint rule and choose **More** > **Delete** in the **Operation** column.
5. Confirm the endpoint rule and click **OK**.

Disassociating a VPC from an Endpoint Rule

1. Go to the **Resolvers** page.
2. Click in the upper left corner and select the desired region and project.
3. Click the **Endpoint Rules** tab to view the endpoint rule list.
4. Locate the endpoint rule and click in the **VPCs** column.



5. In the **Disassociate VPC** dialog box, click **OK**.



6 O&M

6.1 Using CTS to Collect DNS Key Operations

6.1.1 DNS Key Operations Recorded by CTS

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

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

Table 6-1 and **Table 6-2** list the DNS operations that will be recorded by CTS.

NOTE

The DNS service involves resources both at the global and region levels. **Table 6-1** lists DNS operations at the global level. Traces of these operations are displayed only in the primary region.

Table 6-2 lists DNS operations at the region level. Traces of these operations are displayed in the regions where the operations are performed.

Table 6-1 Global-level DNS operations that can be recorded by CTS

Operation	Resource Type	Trace Name	Description
Creating a record set for a public zone	publicRecordSet	createPublicRecord-Set	A record set is added to a public zone.
Deleting a record set from a public zone	publicRecordSet	deletePublicRecord-Set	A record set is deleted from a public zone.
Modifying a record set of a public zone	publicRecordSet	updatePublicRecord-Set	A record set added to a public zone is modified.

Operation	Resource Type	Trace Name	Description
Disabling or enabling a public zone record set	publicRecordSet	updateRecordSetStatus	Disable or enable a record set added a public zone.
Creating a public zone	publicZone	createPublicZone	A public zone is created for hosting a domain name.
Modifying a public zone	publicZone	updatePublicZone	A public zone is modified.
Deleting a public zone	publicZone	deletePublicZone	A public zone is deleted.
Creating a custom line	publicCustomLine	createPublicCustomLine	A custom line is created for a public zone.
Deleting a custom line	publicCustomLine	deletePublicCustomLine	A custom line created for a public zone is deleted.
Modifying a custom line	publicCustomLine	updatePublicCustomLine	A custom line is modified.
Adding a tag to a public zone	publicZoneTag	createPublicZoneTag	A tag is added to a public zone for easier identification.
Deleting a tag from a public zone	publicZoneTag	deletePublicZoneTag	A tag added to a public zone is deleted.
Adding a tag to a record set of a public zone	publicRecordSetTag	createPublicRecordSetTag	A tag is added to a record set of a public zone.
Deleting a tag from a record set of a public zone	publicRecordSetTag	deletePublicRecordSetTag	A tag is deleted from a record set of a public zone.
Creating a PTR record set	ptrRecord	setPTRRecord	A PTR record set is added to a zone.
Resetting a PTR record set	ptrRecord	resetPTRRecord	A PTR record set is reset to delete this record set.

Operation	Resource Type	Trace Name	Description
Deleting a PTR record set	ptrRecord	deletePtrRecord	A PTR record set is deleted.
Adding a tag to a PTR record set	ptrRecordTag	createPTRRecordSet-Tag	A tag is added to a PTR record set.
Deleting a tag from a PTR record set	ptrRecordTag	deletePTRRecordTag	A tag is deleted from a PTR record set.

Table 6-2 Region-level DNS operations that can be recorded by CTS

Operation	Resource Type	Trace Name	Description
Creating a record set in a private zone	privateRecordSet	createPrivateRecord-Set	A record set is added to a private zone.
Deleting a record set from a private zone	privateRecordSet	deletePrivateRecord-Set	A record set is deleted from a private zone.
Modifying a record set of a private zone	privateRecordSet	updatePrivateRe-cordSet	A private zone record set is modified.
Creating a private zone	privateZone	createPrivateZone	A private zone is created for a domain name.
Modifying a private zone	privateZone	updatePrivateZone	A private zone is modified.
Deleting a private zone	privateZone	deletePrivateZone	A private zone is deleted.
Associating a VPC with a private zone	privateZone	associateRouter	A VPC is associated with a private zone.
Disassociating a VPC from a private zone	privateZone	disassociateRouter	A VPC is disassociated from a private zone.
Adding a tag to a private zone	privateZoneTag	createPrivateZone-Tag	A tag is added to a private zone for easier identification.

Operation	Resource Type	Trace Name	Description
Deleting a tag from a private zone	privateZoneTag	deletePrivateZone-Tag	A tag added to a private zone is deleted.
Adding a tag to a record set of a private zone	privateRecordSetTag	createPrivateRecord-SetTag	A tag is added to a record set of a private zone.
Deleting a tag from a record set of a private zone	privateRecordSetTag	deletePrivateRecord-SetTag	A tag is deleted from a record set of a private zone.

6.1.2 Viewing Traces

Scenarios

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

This section describes how to query these records.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner. In the service list, choose **Management & Deployment** > **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. Specify the filters used for querying traces. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

     Select a filter from the drop-down list.

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

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

     If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user who performs operations.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: Specify the start and end time to view traces generated during a time range of the last seven days.
6. Click on the left of the required trace to expand its details.
7. Click **View Trace**.

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

6.2 Access Logging

Scenarios

The requests sent to DNS Resolver are logged in detail, such as the time when a request was sent, client IP address, request path, and server response.

Constraints

To enable access logging, you need to interconnect DNS with LTS and create a log group and a log stream on the LTS console. For details, see the **Log Tank Service User Guide**.

Configuring LTS

Step 1 Create a log group.

1. Go to the **Log Management** page.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Create Log Group**. In the displayed dialog box, enter a name for the log group.

   Set **Log Retention Duration** as needed.
4. Confirm the settings and click **OK**.

Step 2 Create a log stream.

1. On the LTS console, click on the left of the target log group.
2. Click **Create Log Stream**. In the displayed dialog box, enter a name for the log stream.
3. Select an enterprise project as needed.
4. Confirm the settings and click **OK**.

----End

Configuring Access Logging

1. Go to the **Resolvers** page.
2. Click  in the upper left corner and select the desired region and project.
3. Click the **Access Logs** tab.
4. Click **Configure Access Logging**.
5. Configure the parameters, such as **Log Group**, **Log Stream**, and **VPC**, as prompted.
6. Click **OK**.

Viewing Access Logs

1. Go to the **Resolvers** page.
2. Click  in the upper left corner and select the desired region and project.
3. Click the **Access Logs** tab.
4. In the access log list, locate the target access log and click **View Log Details**.

   On the displayed page, view the information about the log group and log stream.
5. Click the name of the log stream and view its details.

   The following is an example log. For details about the fields in the log, see **Table 6-3**. The log format cannot be modified.

```
{
   "content": "2024-07-02 09:28:00.304 baidu.com. A NOERROR TCP cnsouthwest2d _ 192.168.0.138 c1e159ce-ac25-4908-8e31-8ff73ad2f57d",
   "_resource_id": "c1e159ce-ac25-4908-8e31-8ff73ad2f57d",
   "_resource_name": "c1e159ce-ac25-4908-8e31-8ff73ad2f57d",
   "_service_type": "DNS",
   "category": "LTS",
   "collectTime": 1719883683977
}
```

Table 6-3 Fields in a DNS Resolver access log

Field	Description	Value Description	Example Value
content	DNS Resolver access logs	String	2024-07-02 09:28:00.304 baidu.com. A NOERROR TCP cnsouthwest2d _ 192.168.0.138 c1e159ce-ac25-4908-8e31-8ff73ad2f57d
_resource_id	Resource ID	UUID	95c2b814-99dc-939a-e811-ae84c61ea9ee
_resource_name	Resource name	Name of the resource specified by the resource ID	95c2b814-99dc-939a-e811-ae84c61ea9ee
_service_type	Service for which access logs are collected	Fixed value: **DNS**	DNS
category	Log category	Fixed value: **LTS**	LTS
collectTime	LTS log collection time	Integer	1704158708902

Configuring Log Transfer

If you want to analyze access logs later, transfer the logs to OBS for storage.

1. Go to the **Log Transfer** page.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the **Log Transfer** page, click **Configure Log Transfer**.
4. Configure the parameters. For details, see the **Log Tank Service User Guide**.

7 Resource Tags

7.1 Tags

7.1.1 Overview

Scenarios

Tags identify DNS resources such as public zones, private zones, and record sets. You can add tags to resources to facilitate resource identification and management.

You can add up to 20 tags to a cluster during resource creation or add them on the details page of a created resource.

NOTE

If your organization has configured tag policies for the DNS service, you need to add tags to your public zones based on the tag policies. If you add a tag that does not comply with the tag policies, public zones may fail to be created. Contact the administrator to learn more about tag policies.

Basics of Tags

Tags help you identify your cloud resources. When you have many cloud resources of the same type, you can use tags to classify them by dimension (for example, use, owner, or environment).

Figure 7-1 Example tags

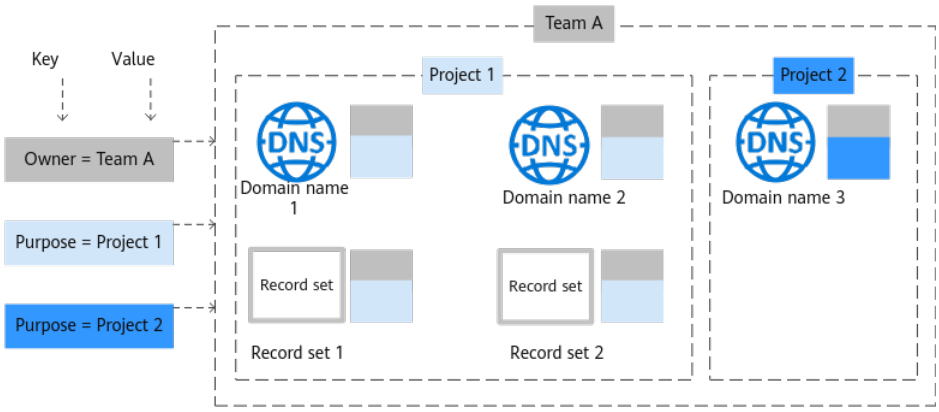


Figure 7-1 shows how tags work. In this example, you assign two tags to each cloud resource. Each tag contains a key and a value that you define. The key of one tag is **Owner**, and the key of another tag is **Usage**. Each tag has a value.

You can quickly search for and filter specific cloud resources based on the tags added to them. For example, you can define a set of tags for cloud resources in an account to track the owner and usage of each cloud resource, making resource management easier.

Tag key and value requirements

- Each tag consists of a key-value pair.
- Each cloud resource can have up to 20 tags.
- For each resource, a tag key must be unique and can have only one tag value.

Tag keys and values must meet the requirements listed in Table 7-1.

Table 7-1 Tag key and value requirements

Parameter	Requirements	Example
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@	example_key1
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and special characters _ . : / = + - @.	example_value1

7.1.2 Public Zone Tags

Scenarios

A tag is the identifier of a private zone. Adding tags to public zones helps you identify and manage your public zones. You can add tags when creating a public zone or add tags to existing public zones. Up to 20 tags can be added to a public zone.

A tag consists of a key and value pair. **Table 7-2** lists the tag key and value requirements.

Table 7-2 Tag key and value requirements

Parameter	Requirements	Example
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@	example_key1
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_value1

Searching for Public Zones by Tag

In the public zone list, search for public zones by tag.

1. Go to the **Public Zones** page.
2. In the search box above the public zone list, select a tag as instructed.

   You can search public zones by tag key or by key-value pair.

   You can add one or more tags. If keys are different, the AND operator is used to filter search results.

   If keys are the same but values are different, the AND operator is used to filter search results.

   – Search by a single tag.

      i. On the **Public Zones** page, select a tag key from the search box.

      ii. Select a tag value for the tag key and start the search.

- Search by multiple tags.

  Repeat **2.i** to **2.ii**, select multiple tag key-value pairs and search for the zones.

Managing Public Zone Tags

You can add, delete, modify, and query tags on the **Tags** tab on the public zone details page.

1. Go to the **Public Zones** page.
2. In the public zone list, click the name of the target zone.
3. Add, delete, modify, and query tags on the **Tags** tab.
   - **Viewing tags**

     On the **Tags** tab, view details about tags such as the number of tags and the key and value of each tag.
   - **Adding a tag**
     i. Click **Add Tag** above the tag list.
     ii. Enter the key and value of the new tag as instructed and click **OK**.
   - **Modifying a tag**
     i. Locate the row that contains the tag and click **Edit** in the **Operation** column.
     ii. Reset the tag key value as instructed and click **OK**.
   - **Deleting a tag**
     i. Locate the row that contains the tag and click **Delete** in the **Operation** column.
     ii. Confirm the information about the tag to be deleted and click **OK**.

7.1.3 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 20 tags can be added to a private zone.

A tag consists of a key and value pair. **Table 7-3** lists the tag key and value requirements.

Table 7-3 Tag key and value requirements

Parameter	Requirements	Example
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@	example_key1
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_value1

Searching for Private Zones by Tag

In the private zone list, search for private zones by tag.

1. Go to the **Private Zones** page.
2. In the search box above the private zone list, select a tag as instructed.

   You can search private zones by tag key or by key-value pair.

   You can add one or more tags. If keys are different, the AND operator is used to filter search results.

   If keys are the same but values are different, the AND operator is used to filter search results.

   - Search by a single tag.
     i. On the **Private Zones** page, select a tag key from the search box.
     ii. Select a tag value for the tag key and start the search.
   - Search by multiple tags.

     Repeat **2.i** to **2.ii**, select multiple tag key-value pairs and search for the zones.

Managing Private Zone Tags

You can add, delete, modify, and query tags on the **Tags** tab on the private zone details page.

1. Go to the **Private Zones** page.
2. Click  in the upper left corner and select the desired region and project.

3. On the **Private Zones** page, click ⌄ to view details about the private zone.
   The details of the private zone are displayed.
4. Add, delete, modify, and query tags on the **Tags** tab.
   - **Viewing tags**
     On the **Tags** tab, view details about tags such as the number of tags and the key and value of each tag.
   - **Adding a tag**
     i. Click **Add Tag** above the tag list.
     ii. Enter the key and value of the new tag as instructed and click **OK**.
   - **Modifying a tag**
     i. Locate the row that contains the tag and click **Edit** in the **Operation** column.
     ii. Reset the tag key value as instructed and click **OK**.
   - **Deleting a tag**
     i. Locate the row that contains the tag and click **Delete** in the **Operation** column.
     ii. Confirm the information about the tag to be deleted and click **OK**.

7.1.4 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 20 tags can be added to a record set.

A tag consists of a key and value pair. **Table 7-4** lists the tag key and value requirements.

Table 7-4 Tag key and value requirements

Parameter	Requirements	Example
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or cannot start with _sys_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@	example_key1

Parameter	Requirements	Example
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Only letters, digits, spaces, and the following special characters are allowed: _.:/=+-@	example_value1

Searching for Record Sets by Tag

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

1. Go to the **DNS console**.
2. On the **Overview** page, click **Record Sets**.
3. Select the **Public Zone Record Sets** or **Private Zone Record Sets** tab.

   Alternatively, on the **Public Zones** or **Private Zones** page, click the domain name to go to the **Record Sets** tab.

   NOTE

   To search for record sets of private zones, click  in the upper left corner of the management console and select a region and project.
4. In the search box above the list, select a tag as instructed.

   You can search zones by tag key or by key-value pair.

   You can add one or more tags. If keys are different, the AND operator is used to filter search results.

   If keys are the same but values are different, the AND operator is used to filter search results.

   – Search by a single tag.

     i. Select a tag key in the search box above the record set list.

     ii. Select a tag value for the tag key and start the search.

   – Search by multiple tags.

     Repeat **4.i** to **4.ii**, select multiple tag key-value pairs, and search for the zones.

Managing Record Set Tags

You can add, delete, modify, and query tags on the **Tags** tab on the record set details page.

1. Go to the **DNS console**.
2. On the **Overview** page, click **Record Sets**.
3. Select the **Public Zone Record Sets** or **Private Zone Record Sets** tab.

   Alternatively, on the **Public Zones** or **Private Zones** page, click the domain name to go to the **Record Sets** tab.

NOTE

To search for record sets of private zones, click in the upper left corner of the management console and select a region and project.

4. In the upper right corner of the record set list, click and select **Tag**.
5. In the **Tag** column of the target record set, add, delete, modify, and view tags.
   - **Viewing tags**
     In the **Tag** column of the target record set, view details about tags such as the number of tags and the key and value of each tag.
   - **Adding, editing, and deleting tags**
     i. Click next to the tag of the target record set.
     ii. Add, edit, and delete tags as instructed.

7.2 Quota Adjustment

What Is Quota?

Quotas put limits on the quantities and capacities of resources available to users. Private and public zones, PTR records, 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. Click in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Quotas** 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?

1. Log in to the **management console**.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Quotas** page is displayed.
3. Click **Increase Quota** in the upper right corner of the page.
4. On the **Create Service Ticket** page, configure parameters as required.
   In the **Problem Description** area, fill in the content and reason for adjustment.

5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

