

Domain Name Service

User Guide

Issue 01
Date 2025-02-28



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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 Public Zones.....	1
1.1 Public Zone Overview.....	1
1.2 Creating a Public Zone.....	2
1.3 Managing Public Zones.....	5
1.4 Reclaiming a Public Zone.....	8
1.5 Checking a Domain Name.....	9
1.6 Changing DNS Servers for a Public Domain Name.....	10
1.7 Configuring DNSSEC.....	11
2 Private Zones.....	14
2.1 Private Zone Overview.....	14
2.2 Creating a Private Zone.....	15
2.3 Managing Private Zones.....	19
2.4 Sharing a Private Zone.....	21
2.5 Associating a VPC with a Private Zone.....	24
2.6 Disassociating a VPC from a Private Zone.....	24
2.7 Configuring Recursive Resolution for Subdomains.....	25
3 Record Sets.....	28
3.1 Record Set Overview.....	28
3.2 Adding Record Sets.....	30
3.2.1 Record Set Types and Configuration Rules.....	30
3.2.2 Adding an A Record Set.....	36
3.2.3 Adding a CNAME Record Set.....	40
3.2.4 Adding an MX Record Set.....	43
3.2.5 Adding an AAAA Record Set.....	47
3.2.6 Adding a TXT Record Set.....	50
3.2.7 Adding an SRV Record Set.....	55
3.2.8 Adding an NS Record Set.....	58
3.2.9 Adding a CAA Record Set.....	61
3.2.10 Adding a PTR Record Set.....	65
3.3 Disabling or Enabling Record Sets.....	67
3.4 Managing Record Sets.....	68
3.5 Configuring a Wildcard DNS Record Set.....	70

3.6 Searching for Record Sets.....	73
3.7 Importing Record Sets.....	73
3.8 Exporting Record Sets.....	74
3.9 Migrating to Huawei Cloud DNS for Domain Name Resolution.....	75
4 PTR Records.....	78
4.1 PTR Record Overview.....	78
4.2 Creating a PTR Record.....	79
4.3 Managing PTR Records.....	82
5 Intelligent Resolution.....	84
5.1 Intelligent Resolution Overview.....	84
5.2 Configuring ISP Lines.....	85
5.3 Configuring Region Lines.....	90
5.4 Configuring Custom Lines.....	96
5.5 Configuring Weighted Routing.....	100
6 Resolver.....	103
6.1 DNS Resolver Overview.....	103
6.2 Managing Inbound Endpoints.....	104
6.3 Managing Outbound Endpoints.....	106
6.4 Managing Endpoint Rules.....	108
6.5 Sharing an Endpoint Rule.....	111
7 Permissions Management.....	115
7.1 Creating a User and Granting DNS Permissions.....	115
7.2 Creating Custom Policies.....	116
8 Using CTS to Collect DNS Key Operations.....	119
8.1 DNS Key Operations Recorded by CTS.....	119
8.2 Viewing Traces.....	122
9 Access Logging.....	124
10 Quota Adjustment.....	128

1 Public Zones

1.1 Public Zone Overview

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

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

Table 1-1 Public zone operations

Operation	Scenario	Constraints
Creating a Public Zone	Create a zone for your domain name.	<ul style="list-style-type: none">Public zones are global resources. You do not need to select a region or project.Each account can have up to 50 public zones.
Managing Public Zones	Modify, delete, enable, disable, and view public zones.	<ul style="list-style-type: none">The domain name of a created public zone cannot be modified.If a public zone is deleted, all its record sets will also be deleted.If a public zone is disabled, all its record sets will not take effect.

Operation	Scenario	Constraints
Reclaiming a Public Zone	Reclaim a public zone by proving that you are the holder of the domain name to Huawei Cloud when message "This public zone has been created by another account" is displayed when you create a public zone.	<ul style="list-style-type: none">• The domain name has already been registered with a third party registrar.• Only the domain name holder can reclaim the public zone.
Configuring DNSSEC	Use digital signatures to ensure the authenticity and integrity of DNS response packets, protect end users from being redirected to unexpected addresses, and prevent attacks such as DNS spoofing and cache pollution.	<ul style="list-style-type: none">• DNSSEC does not support subdomains.• Before disabling DNSSEC, delete the DS record from the domain name service provider.• When transferring DNS record sets across accounts on the DNS console, you need to delete the DS record from the domain name service provider and then disable DNSSEC on the DNS console. Otherwise, the resolution may fail.• Before transferring a domain name across accounts on the Domains console, you need to delete the DS record and then disable DNSSEC on the DNS console, or DNS resolution may fail.

1.2 Creating a Public Zone

Scenarios

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

Prerequisites

You have registered a domain name.

Procedure

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

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

3. Configure the parameters.

Figure 1-1 Creating a public zone

Table 1-2 describes the parameters.

Table 1-2 Parameters for creating a public zone

Parameter	Description	Example Value
Domain Name	Name of the public zone, which is the domain name you have registered with a domain name registrar. For details about the domain name format, see Domain Name Format and DNS Hierarchy .	example.com

Parameter	Description	Example Value
Enterprise Project	<p>Enterprise project associated with the public zone.</p> <p>You can manage public zones by enterprise project.</p> <p>NOTE This parameter is available and mandatory only when Account Type is set to Enterprise Account.</p> <p>When setting this parameter, note the following:</p> <ul style="list-style-type: none"> • If you do not manage zones by enterprise project, select the default enterprise project. • If you manage zones by enterprise project, select an existing enterprise project. 	default
Tag	<p>(Optional) Identifier of the zone.</p> <p>Each tag contains a key and a value. You can add up to 20 tags to a zone.</p> <p>For details about tag key and value requirements, see Table 1-3.</p> <p>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.</p>	example_key1 example_value1
Description	<p>(Optional) Supplementary information about the zone.</p> <p>The description can contain no more than 255 characters.</p>	This is a zone example.

Table 1-3 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each resource.• Can contain no more than 36 characters.• Cannot start or end with a space nor contain special characters =* <> \, /	example_key1
Value	<ul style="list-style-type: none">• Cannot be left blank.• Can contain no more than 43 characters.• Cannot start or end with a space nor contain special characters =* <> \, /	example_value1

4. Click **OK**.

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

5. Click the domain name or click **Manage Record Sets** in the **Operation** column.

On the **Record Sets** tab, click **Add Record Set**. For details about the parameters, see [Record Set Overview](#).

NOTE

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

- The SOA record set includes administrative information about your zone, as defined by the Domain Name System (DNS).
- The NS record set defines the authoritative DNS servers for the domain name. You can modify the NS record set based on the region of the domain name. For more information about the DNS servers, see [What Are Huawei Cloud DNS Servers?](#)

Follow-up Operations

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

- Add record sets for it. For details, see [Record Set Overview](#).
- Modify or delete it, or view its details. For details, see [Managing Public Zones](#).

1.3 Managing Public Zones

Scenarios

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

Modifying a Public Zone

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

NOTE

For more information about the email 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**.

Transferring a Public Zone

You can transfer a public zone including all its record sets from one account to another.

1. Go to the [Public Zones](#) page.
2. Locate the public zone you want to transfer, choose **More > Transfer** in the **Operation** column.

The **Transfer Public Zones** tab is displayed.

3. Enter the ID of the account that you want to transfer the domain name to.
4. Click **Submit**.

Deleting a Public Zone

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

NOTICE

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

1. 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**.

Deleting Public Zones

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

NOTICE

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

1. Go to the [Public Zones](#) page.
2. Select the public zones you want to delete and click **Delete**.
3. In the displayed dialog box, confirm the public zones to be deleted.
Enter **DELETE** and click **OK**.

Disabling or Enabling a Public Zone

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

View details about a public zone, such as zone ID, operation time (creation time and last modification time), tag, and TTL, on the [Public Zones](#) page.

1. Go to the [Overview](#) page.
2. On the [Overview](#) page, click **Public Zones** under **My Resources**.

Exporting Public Zones

You can export all or selected public zones to an XLSX file.

1. Go to the [Public Zones](#) page.
2. In the upper part of the public zone list, click **Export**.
3. Select the public zones to be exported:
 - All public zones
 - Only selected public zones

Figure 1-2 Exporting public zones

The screenshot shows a management interface for public zones. At the top, there are buttons for 'Delete' and 'Batch Operation', and an 'Export' button. Below these is a search bar and a dialog box titled 'Export all data to an XLSX file' with the option 'Export selected data to an XLSX file'. The main part of the interface is a table with the following columns: Domain Name, DNS ID, Email, TTL (s), Created, Last Modified, Description, Enterprise Project, and Operation. The table contains five rows of data for different domains.

Domain Name	DNS ID	Email	TTL (s)	Created	Last Modified	Description	Enterprise Project	Operation
ample.com	11		300	Aug 06, 2024 11:05:3...	Aug 06, 2024 11:05...			Manage Record Set Check Domain Name Disable More
ample.com	3		300	Jul 26, 2024 16:05:13...	Jul 26, 2024 16:05...			Manage Record Set Check Domain Name Disable More
ample.com	2		300	Sep 27, 2023 10:53:1...	Sep 27, 2023 10:5...			Manage Record Set Check Domain Name Disable More
ample.com	12		300	Sep 26, 2023 17:08:2...	Sep 26, 2023 17:0...			Manage Record Set Check Domain Name Disable More
ample.com	2		300	Sep 08, 2023 11:31:11...	Sep 08, 2023 11:31...			Manage Record Set Check Domain Name Disable More

1.4 Reclaiming a Public Zone

Scenarios

If you are the holder of a domain name and "This public zone has been created by another account. You need to reclaim it first." is displayed when you **create a public zone** for your domain name on the DNS console, you can reclaim the public zone.

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 holder and your public zone will be reclaimed automatically.

You can perform the following operations to reclaim a public zone.

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.
-

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 another DNS service provider's platform and are for reference only. For details, see the documentation of that DNS service provider.

1. Log in to the management console of the third-party DNS service provider.
2. In the public zone list, locate the public zone and click the domain name.
The page for you to configure the record is displayed.
3. 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**.

4. 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

1.5 Checking a Domain Name

Scenarios

After you add record sets on the Huawei Cloud DNS console, you can check whether they are active. If they are not, Huawei Cloud DNS provides you with suggestions to address the issue.

Constraints

Only record sets added to public zones can be checked.

Checking a Website Domain Name

After configuring all required record sets for a website domain name, you can perform the following operations to check whether these record sets are active:

1. Go to the [Public Zones](#) page.
2. Locate the target public zone and click **Check Domain Name** in the **Operation** column.
The **Check Domain Name** dialog box is displayed.
3. On the **Domain Names** tab, locate the domain name and click **Start Check** in the **Operation** column.
The A, AAAA, and CNAME record sets configured for the domain name will be checked in sequence.
4. View the check result and rectify the fault using the provided solution.

Checking an Email Domain Name

After configuring all required record sets for an email domain name, you can perform the following operations to check whether these record sets are active:

1. Go to the [Public Zones](#) page.
2. Locate the target public zone and click **Check Domain Name** in the **Operation** column.
3. In the **Check Domain Name** dialog box, click **Email Domains**.
4. Click **Start Check**.
5. View the check result and rectify the fault using the provided solution.
You can also click **View Details** to view detailed information.

Common Issues and Solutions

Error Message	Possible Causes	Solution
The domain name cannot be resolved.	The DNS settings for the domain name do not take effect.	Contact your domain name registrar to check the domain name status.
	The domain name has not been registered yet.	Register the domain name with a domain name registrar.
	The request timed out or the task failed.	Try again later.
The domain name is not hosted on Huawei Cloud DNS.	The domain name is managed by another DNS service provider.	Configure record sets on the console of that DNS service provider or contact that DNS service provider for troubleshooting.

1.6 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.com: DNS server for regions in the Chinese mainland
- ns1.huaweicloud-dns.cn: DNS server for regions in the Chinese mainland
- ns1.huaweicloud-dns.net: DNS server for countries or regions outside the Chinese mainland

- ns1.huaweicloud-dns.org: DNS server for countries or regions outside the Chinese mainland

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.

1.7 Configuring DNSSEC

What Is DNSSEC?

DNS Security Extensions (DNSSEC) provides digital signatures to ensure data integrity and authenticity of DNS requests and responses and to defend against common attacks such as DNS spoofing. This prevents you from being redirected to unexpected addresses and protects your core services.

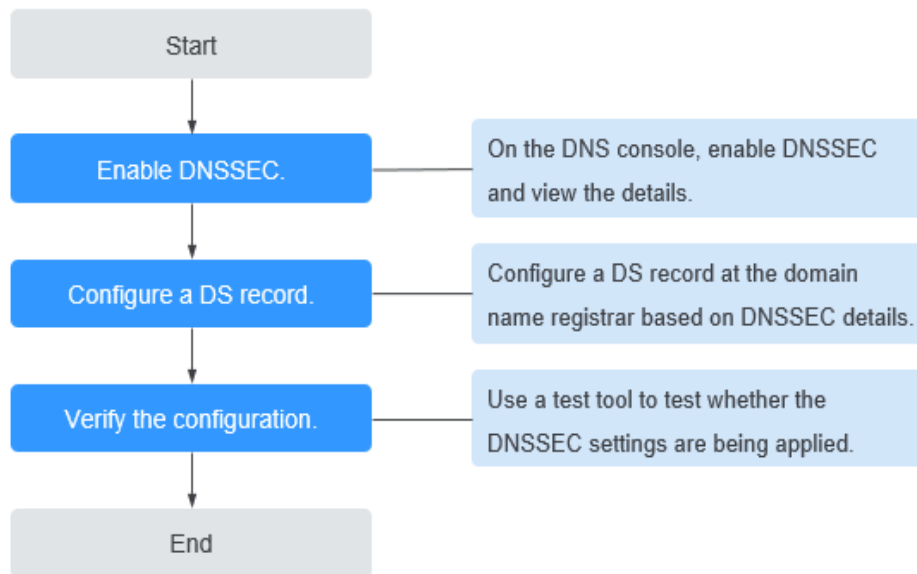
Constraints

- To use DNSSEC, both the domain name registrar and the DNS service provider must support DNSSEC.
- DNSSEC does not support subdomains.
- Before disabling DNSSEC, you need to delete the DS record from the domain name service provider's system.
- Before transferring the record sets across accounts on the DNS console, you need to delete the DS record from the domain name registrar and then disable DNSSEC on the DNS console, or DNS resolution may fail.
- Before transferring a domain name across accounts on the Domains console, you need to delete the DS record and then disable DNSSEC on the DNS console, or DNS resolution may fail.
- CNAME record sets cannot be configured for the second-level domain name, or the domain name cannot be resolved normally.

Process Flow

Figure 1-3 shows the process of configuring DNSSEC for a public zone

Figure 1-3 DNSSEC configuration process

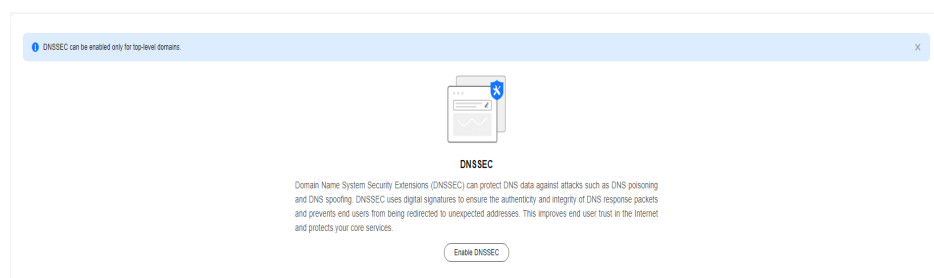


Procedure

Step 1 Enable DNSSEC.

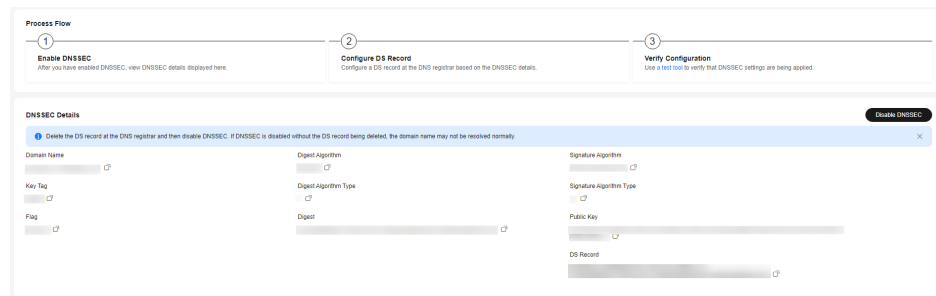
1. Go to the **Public Zones** page.
2. Locate the public zone for which you want to enable DNSSEC and click the domain name.
The **Record Sets** tab is displayed.
3. Click the **DNSSEC** tab.
4. Click **Enable DNSSEC**.

Figure 1-4 Enabling DNSSEC



5. View and take a note of the following DNSSEC information:
Key tag, digest algorithm, digest algorithm type, and digest.

Figure 1-5 Viewing DNSSEC details



6. Go to the domain name registrar to configure a DS record.

Step 2 Configure a DS record.

The following are operations for domain names that are not registered with Huawei Cloud and are only for reference. For details, see the operation guide on the official website of the domain name registrar.

1. Log in to the management console.
2. In the public zone list, locate the public zone and click **More > Manage** in the **Operation** column.
3. Click **DNSSEC**.
4. Click **Add DS Record**.
5. Configure the parameters as prompted and enter the DNSSEC information recorded in **Step 1.5**.
 - **Key Tag**: Enter the recorded key tag.
 - **Algorithm**: Enter the recorded signature algorithm type and signature algorithm.
Format: Signature algorithm type-Signature algorithm
 - **Digest Type**: Enter the recorded digest algorithm type and digest algorithm.
Format: Digest algorithm type-Digest algorithm
 - **Digest**: Enter the recorded digest.
6. Click **OK**.

----End

Verification

Use the **test tool** to verify that the configuration has taken effect.

2 Private Zones

2.1 Private Zone Overview

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

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

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

[Table 2-1](#) describes the operations that you can perform on private zones.

Table 2-1 Private zone operations

Operation	Scenario	Constraints
Creating a Private Zone	Create a private zone for your domain name.	<ul style="list-style-type: none">Private zones are project-level resources. When you create a private zone, select a region and project.Each account can create up to 50 private zones.Private domain names must meet the following requirements:<ul style="list-style-type: none">Domain name labels are separated by period (.), and each label does not exceed 63 characters.A domain name label can contain letters, digits, and hyphens (-) and cannot start or end with a hyphen.The total length of a domain name cannot exceed 254 characters.
Managing Private Zones	Modify, delete, batch delete, and view private zones.	<ul style="list-style-type: none">The domain name of a created private zone cannot be modified.If a private zone is deleted, all its record sets will also be deleted.
Associating a VPC with a Private Zone	Associate a VPC with a private zone.	<ul style="list-style-type: none">You can only associate VPCs that you have created using your own account.Each VPC can be associated only with one private zone. However, a private zone can have more than one VPC associated with it.
Disassociating a VPC from a Private Zone	Disassociate a VPC from a private zone.	<ul style="list-style-type: none">After the disassociation, private domain names will not take effect in the VPC.If a private zone is only associated with one VPC, you cannot disassociate it.

2.2 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.

Constraints

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

associated with the private zone cannot conflict with the 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.

Procedure

1. Go to the [Private Zones](#) page.
2. In the upper right corner of the page, click **Create Private Zone**.
3. Configure the parameters.

Figure 2-1 Creating a private zone

Create Private Zone ✕

* Domain Name
Example: example.com

Recursive resolution proxy for subdomains ?

* Region

* VPC [View VPCs](#)
Select a VPC that you want to associate with the private zone. Only ECSs in associated VPCs can access the private zone.

* Enterprise Project [Create Enterprise Project](#)

Tag
It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) ?
To add a tag, enter a tag key and a tag value below.

Enter a tag key Enter a tag value

Tags you can still add: 20

Description 0/255 ↗

[Table 2-2](#) describes the parameters.

Table 2-2 Parameters for creating a private zone

Parameter	Description	Example Value
Domain Name	<p>Domain name you have planned for the ECS.</p> <p>You can enter a top-level domain that complies with the domain naming rules.</p> <p>For details about the domain name format, see Domain Name Format and DNS Hierarchy.</p>	example.com
Recursive resolution proxy for subdomains	<p>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.</p>	-
Region	<p>Region of the VPC associated with the private zone.</p>	CN-Hong Kong
VPC	<p>VPC to be associated with the private zone.</p> <p>NOTE This VPC you choose must be the VPC where your servers (such as ECSs) are. Otherwise, the domain name cannot be resolved.</p>	-
Email	<p>(Optional) Email address of the administrator managing the private zone.</p> <p>Recommended email address: HOSTMASTER@Domain name</p> <p>For more information about the email address, see Why Was the Email Address Format Changed in the SOA Record?</p>	HOSTMASTER@example.com

Parameter	Description	Example Value
Tag	<p>(Optional) Identifier of the zone. 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 2-3.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your private zones based on the tag policies. If you add a tag that does not comply with the tag policies, private zones may fail to be created. Contact the administrator to learn more about tag policies.</p>	<p>example_key1 example_value1</p>
Description	<p>(Optional) Supplementary information about the zone. The description can contain no more than 255 characters.</p>	<p>This is a zone example.</p>

Table 2-3 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =* < > \, / 	<p>example_key1</p>
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =* < > \, / 	<p>example_value1</p>

- Click **OK**.
- Switch back to the **Private Zones** page.
You can view the created private zone on the **Private Zones** page.
- Click the domain name to add record sets.
On the **Record Sets** tab, click **Add Record Set**. For details about the parameters, see [Record Set Overview](#).

 **NOTE**

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

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

Follow-up Operations

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

- Add record sets for it. For more information about record sets, see [Record Set Overview](#).
- Modify or delete the private zone, or view its details. For details, see [Managing Private Zones](#).

2.3 Managing Private Zones

Scenarios

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

Modifying a Private Zone

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

 **NOTE**

For more information about the email address, see [Why Was the Email Address Format Changed in the SOA Record?](#)

1. Go to the [Private Zones](#) page.
2. Locate the private zone you want to modify and choose **More > Modify** in the **Operation** column.
The **Modify Private Zone** dialog box is displayed.

3. Modify the private zone.
4. 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 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**.

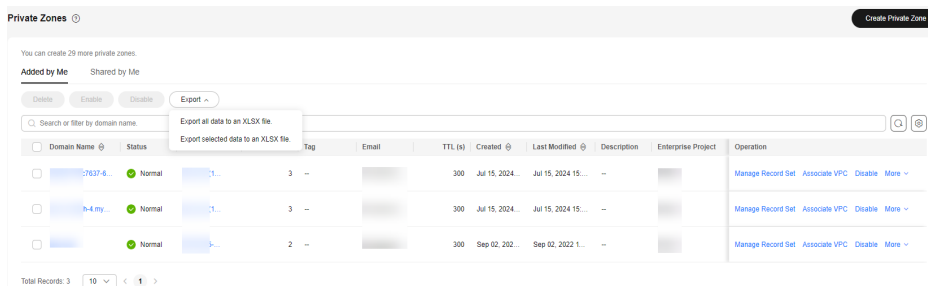
Exporting Private Zones

You can export all or selected private zones to an XLSX file.

1. Go to the [Private Zones](#) page.
2. In the upper part of the private zone list, click **Export**.
3. Select the private zones to be exported:

- All private zones
- Only selected private zones

Figure 2-2 Exporting private zones



2.4 Sharing a Private Zone

Overview

DNS can work with Resource Access Manager (RAM) to allow you to share your private zones to other accounts if you are the owner of these private zones. When a resource owner shares resources with your account and you accept the resource sharing invitation, you can access and use the shared resources as if they were your own resources in your own account. Resource owners can select different permissions based on the principle of least privilege (PoLP) and service requirements, and principals can only access resources within their permissions. This improves resource security. For more information about RAM, see [What Is Resource Access Manager?](#)

If your account is managed by Huawei Cloud Organizations, you can enable sharing with Organizations to share resources more easily. If your account is in an organization, you can share resources either with individual accounts or with all accounts in the organization or in an organization unit (OU) without the need to enumerate each account. For details, see [Enabling Sharing with Organizations](#).

Resource and Region Availability

[Table 2-4](#) lists the resources that can be shared and regions where resource sharing is supported.

Table 2-4 Resources that can be shared and regions where resource sharing is supported

Cloud Service	Resource Type	Regions
DNS	Private zones	CN East-Qingdao CN South-Guangzhou CN-Hong Kong AP-Singapore AP-Bangkok AP-Jakarta TR-Istanbul AF-Johannesburg ME-Riyadh CN East2

Constraints

- You cannot share a private zone that is shared with your account. Only resource owners can share the resources in their accounts with other accounts.
- If you share a private zone with your organization or an OU, you must enable sharing with Organizations. For details, see [Enabling Sharing with Organizations](#).
- A principal can accept up to 50 private zones from resource owners.
- A private zone that is no longer shared with you will not be displayed on the **Shared with Me** tab. If you have associated a VPC with that private zone, the private domain name can still be resolved within that VPC. To disassociate the VPC from the private zone, the account that shared the private zone needs to share the private zone with you again.

Creating a Share

1. Go to the [Private Zones](#) page.
2. Go to the **Created by Me** tab, locate the private zone you want to share, and click **Share** in the **Operation** column.
3. On the **Create Resource Share** page, specify the resource to be shared, configure permissions, and specify users as prompted.

For details, see [Creating a Resource Share](#).

NOTE

After an owner shares a private zone with a principal, the principal needs to accept the sharing within a specified period. For details, see [Responding to a Resource Sharing Invitation](#).

Viewing Share Details

1. Go to the [Private Zones](#) page.
2. Go to the **Shared with Me** tab and view the private zones that are shared with your account.

NOTE

- If you are the owner of a shared private zone, you can view the shared private zone, permissions, and principals on the RAM management console. For details, see [Viewing a Resource Share](#).
- If you are a principal of a shared private zone, you can view the shared private zone, permissions, and resource owner on the RAM management console. For details, see [Viewing Resources Shared with You](#).

Stopping a Share

- If a share is no longer needed, you can delete it at any time as the owner. Deleting a share does not delete the shared resources. After a share is deleted, the principals will no longer use the shared resources. For details, see [Deleting a Resource Share](#).
- If you are a principal and you do not need to access the shared resources, you can leave a resource share at any time. After you leave a resource share, you lose access to the shared resources.

You can leave a resource share only if the resources were shared with you as an individual Huawei Cloud account and not as part of an organization. You cannot leave a resource share if you were added to it by an account inside your organization and sharing with Organizations is enabled. For details, see [Leaving a Resource Share](#).

Operation Permissions on Shared Private Zones

The owner and principals of a shared private zone have different operation permissions on the private zone and associated resources. For details, see [Table 2-5](#).

Table 2-5 Operation permissions on shared private zones and associated resources

Resource	Owner	Principal
Private zone	Has all operation permissions on the shared private zones.	Can only view the VPCs that are associated with the shared private zones, but cannot perform any operations on the VPCs.

Billing

N/A

2.5 Associating a VPC with a Private Zone


Scenarios

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

NOTE

This VPC 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.

Figure 2-3 Associated VPCs

<input type="checkbox"/>	Domain Name	Status	Record Sets	Associated VPC	Description	Operation
<input type="checkbox"/>	example.com	● Normal	2	vpc vpc	--	Manage Record Set Associate VPC More ▾

2.6 Disassociating a VPC from a Private Zone

Scenarios



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

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**.

2.7 Configuring Recursive Resolution for Subdomains

Scenarios

You can enable the recursive resolution proxy option for private zones.

After this option is enabled, if no record sets are configured for the subdomain, the DNS service does not directly return **nxdomain** (which means that no record sets are configured). Instead, the DNS queries are forwarded to the Internet for resolution.

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 2-6 Record sets

Name	Type	Value
a1	A	1.2.3.4

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

When you access www.example.com, 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](#).

Figure 2-4 Enabling recursive subdomain resolution when creating a private zone

Create Private Zone ✕

* Domain Name
Example: example.com

Recursive resolution proxy for subdomains ?

* Region

* VPC [View VPCs](#)
Select a VPC that you want to associate with the private zone. Only ECSs in associated VPCs can access the private zone.

* Enterprise Project [Create Enterprise Project](#)

Tag
It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#)
To add a tag, enter a tag key and a tag value below.

Enter a tag key Enter a tag value

Tags you can still add: 20

Description 0/255 ↕

- **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](#).

Figure 2-5 Enabling recursive subdomain resolution when modifying a private zone

Modify Private Zone ×

Domain Name

Recursive resolution proxy for subdomains ?

Email

Enter the domain name administrator's email address, which will be used in the SOA record for the zone. If you leave it empty, the system will automatically specify one for you.

Description

0/255 ↵

3 Record Sets

3.1 Record Set Overview

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

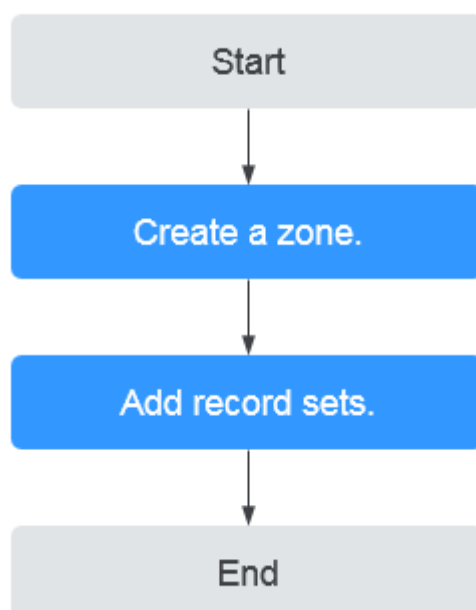
Table 3-1 Record set management

Operation	Scenario	Constraints
Adding Record Sets	View record set types supported by the DNS service and their configuration rules, and configure record sets for a domain name. For details, see Table 3-2 .	<ul style="list-style-type: none"> After a zone is created for a domain name, SOA and NS record sets are automatically created. Up to 500 record sets can be added by an account.
Managing Record Sets	Modify, delete, and view record sets.	<ul style="list-style-type: none"> After a record set is added, its resolution line cannot be modified. You can modify the TTL, value, and description of the NS record set that is automatically generated. You cannot modify the value of the SOA record set that is automatically generated. You cannot delete or disable SOA and NS record sets that are automatically generated.
Configuring a Wildcard DNS Record Set	Add a record set that matches all subdomains.	Wildcard DNS resolution does not support NS and SOA record sets.

Operation	Scenario	Constraints
Searching for Record Sets	Search for, modify, disable, and delete record sets on the Overview > Record Sets page.	None
Importing Record Sets	Batch import record sets.	<ul style="list-style-type: none"> Record sets are listed in .xlsx files, and each file cannot exceed 2 MB. Up to 500 record sets can be imported at a time.
Exporting Record Sets	Batch export record sets.	None
Migrating to Huawei Cloud DNS for Domain Name Resolution	Migrate an in-use domain name to Huawei Cloud.	<ul style="list-style-type: none"> Before the migration, obtain all record sets from your current DNS service provider. After the migration, change the DNS servers of the domain name to those provided by Huawei Cloud DNS in the domain name registrar's system.

Figure 3-1 shows the process for configuring a record set on the DNS console.

Figure 3-1 Process for configuring a record set



 NOTE

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

- [Creating a Public Zone](#)
- [Creating a Private Zone](#)

3.2 Adding Record Sets

3.2.1 Record Set Types and Configuration Rules

Record Set Types

[Table 3-2](#) describes the record set types.

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

Table 3-2 Record set types

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

Record Set Type	Description	Value	Example
MX	Maps domain names to email servers.	<p>Email server address</p> <p>You can enter up to 50 different IP addresses, each on a separate line.</p> <p>The format is [priority][mail server host name].</p> <p>Configuration rules:</p> <ul style="list-style-type: none"> • 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 	<p>10 mailserver.example.com.</p> <p>20 mailserver2.example.com.</p>
AAAA	Maps domain names to IPv6 addresses.	<p>IPv6 addresses mapped to the domain name.</p> <p>You can enter up to 50 different IP addresses, each on a separate line.</p>	<p>ff03:0db8:85a3:0:0:8 a2e:0370:7334</p>

Record Set Type	Description	Value	Example
<p>TXT</p>	<p>Creates text records for domain names. It is usually used in the following scenarios:</p> <ul style="list-style-type: none"> • To record DKIM public keys to prevent email fraud. • To record the identity of domain name owners to facilitate domain name retrieval. 	<p>Text content</p> <p>Configuration rules:</p> <ul style="list-style-type: none"> • Text record values must be enclosed in double quotation marks. • One or more text record values are supported, each on a separate line. A maximum of 50 text record values can be entered. • A single text record value can contain multiple character strings, each of which is double quoted and separated from others using a space. One character string cannot exceed 255 characters. A value must not exceed 4096 characters. • The value cannot be left blank. • The text cannot contain a backslash (\). 	<ul style="list-style-type: none"> • 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	Value	Example
<p>SRV</p>	<p>Records servers providing specific services.</p>	<p>Server address</p> <p>You can enter up to 50 different IP addresses, each on a separate line.</p> <p>The value format is [priority] [weight] [port number] [server address].</p> <p>Configuration rules:</p> <ul style="list-style-type: none"> • The priority, weight, and port number range from 0 to 65535. • A smaller value indicates a higher priority. • A larger value indicates a larger weight. • The server address is the domain name of the target server. Ensure that the domain name can be resolved. <p>NOTE</p> <p>If the record set values have the same priority, requests to the domain name will be routed based on weights.</p>	<p>2 1 2355 example_server.test.com</p>

Record Set Type	Description	Value	Example
<p>NS</p>	<p>Delegates subdomains to other name servers.</p> <ul style="list-style-type: none"> • For public zones, an NS record set is automatically created, and you can add NS record sets for subdomains. • For private zones, an NS record set is automatically created, and you cannot add other NS record sets. 	<p>DNS server address</p> <p>You can enter up to 50 different IP addresses, each on a separate line.</p>	<p>ns1.example.net ns2.example.net</p>
<p>SOA</p>	<p>Identifies the base information about a domain name. The SOA record set is automatically generated by the DNS service and cannot be added manually.</p>	<p>This type of record set is created by default and cannot be added manually.</p>	<p>This type of record set is created by default and cannot be added manually.</p>

Record Set Type	Description	Value	Example
CAA	<p>Grants certificate issuing permissions to certificate authorities (CAs). CAA record sets can prevent the issuance of unauthorized HTTPS certificates.</p>	<p>CA to be authorized to issue certificates for a domain name or its subdomains</p> <p>You can enter up to 50 different IP addresses, each on a separate line.</p> <p>The format is [flag] [tag] [value].</p> <p>Configuration rules:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> - issue: authorizes a CA to issue all types of certificates. - issuewild: authorizes a CA to issue wildcard certificates. - iodef: requests notifications 	<p>0 issue "ca.abc.com"</p> <p>0 issuewild "ca.def.com"</p> <p>0 iodef "mailto:admin@domain.com"</p> <p>0 iodef "http://domain.com/log/"</p>

Record Set Type	Description	Value	Example
		<p>once a CA receives invalid certificate requests.</p> <ul style="list-style-type: none"> 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 no more than 255 characters. Only letters, digits, spaces, and special characters -#*? &_~=:;.@+^/!% are allowed. 	
PTR	Maps IP addresses to domain names.	Private domain name mapped to the private IP address. You can enter only one domain name.	www.example.com

3.2.2 Adding an A Record Set

Scenarios

If you want end users to use a domain name to access your website, web application, or cloud server with an IPv4 address bound, configure an A record set for this domain name.

For more information about each type of record sets, see [Record Set Types and Configuration Rules](#).

Prerequisites

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

Procedure


1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**. The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. Locate the zone and click **Manage Record Sets** in the **Operation** column.
5. Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.
6. Configure the parameters based on [Table 3-3](#).

Table 3-3 Parameters for adding an A record set

Parameter	Description	Example Value
Type	Type of the record set. A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone. For details, see Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?	A – Map domains to IPv4 addresses

Parameter	Description	Example Value
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> • www: The domain name is <code>www.example.com</code>, which is usually used for a website. • Left blank: The domain name is <code>example.com</code>. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • abc: The domain name is <code>abc.example.com</code>, a subdomain of <code>example.com</code>. • mail: The domain name is <code>mail.example.com</code>, which is usually used for email servers. • *: The domain name is <code>*.example.com</code>, which is a wildcard domain name, indicating all subdomains of <code>example.com</code>. 	www
Line	<p>Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return.</p> <p>The default value is Default.</p> <p>This parameter is only configurable for public zone record sets.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • 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)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	300

Parameter	Description	Example Value
Value	IPv4 addresses mapped to the domain name. You can enter up to 50 different IP addresses, each on a separate line.	192.168.12.2 192.168.12.3
Weight	(Optional) Weight for the record set. The value ranges from 0 to 1000 , and the default value is 1 . This parameter is only configurable for public zone record sets. 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	(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set. For details about tag key and value requirements, see Table 3-4 . NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set. The description can contain no more than 255 characters.	-

Table 3-4 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =* <> \, / 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =* <> \, / 	example_value1

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

Related Operations

For details about how to configure A record sets, see [Routing Internet Traffic to a Website](#).

3.2.3 Adding a CNAME Record Set

Scenarios

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

For more information about each type of record sets, see [Record Set Types and Configuration Rules](#).

Constraints

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

Procedure


1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**.
The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. Locate the zone and click **Manage Record Sets** in the **Operation** column.
5. Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.
6. Configure the parameters based on [Table 3-5](#).

Table 3-5 Parameters for adding a CNAME record set

Parameter	Description	Example Value
Type	<p>Type of the record set</p> <p>A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone.</p> <p>For details, see Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?</p>	CNAME – Map one domain to another
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> • www: The domain name is www.example.com, which is usually used for a website. • Left blank: The domain name is example.com. 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, which is usually used for email servers. • *: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com. 	Left blank

Parameter	Description	Example Value
Line	<p>Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return.</p> <p>The default value is Default.</p> <p>This parameter is only configurable for public zone record sets.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • 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)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	300
Value	Domain name alias. You can enter only one domain name.	webserver01.example.com
Weight	<p>(Optional) Weight for the record set. The value ranges from 0 to 1000, and the default value is 1.</p> <p>This parameter is only configurable for public zone record sets.</p> <p>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.</p>	1

Parameter	Description	Example Value
Tag	<p>(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 3-6.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.</p>	example_key1 example_value1
Description	<p>(Optional) Supplementary information about the record set.</p> <p>The description can contain no more than 255 characters.</p>	-

Table 3-6 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =*<>\\, / 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =*<>\\, / 	example_value1

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

3.2.4 Adding an MX Record Set

Scenarios

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

For more information about each type of record sets, see [Record Set Types and Configuration Rules](#).

Prerequisites

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

Procedure


1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**. The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. Locate the zone and click **Manage Record Sets** in the **Operation** column.
5. Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.
6. Configure the parameters based on [Table 3-7](#).

Table 3-7 Parameters for adding an MX record set

Parameter	Description	Example Value
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> • www: The domain name is <code>www.example.com</code>, which is usually used for a website. • Left blank: The domain name is <code>example.com</code>. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • abc: The domain name is <code>abc.example.com</code>, a subdomain of <code>example.com</code>. • mail: The domain name is <code>mail.example.com</code>, which is usually used for email servers. • *: The domain name is <code>*.example.com</code>, which is a wildcard domain name, indicating all subdomains of <code>example.com</code>. 	Left blank
Type	<p>Type of the record set</p> <p>A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone.</p> <p>For details, see Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?</p>	MX – Map domains to email servers

Parameter	Description	Example Value
Line	<p>Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return. The default value is Default.</p> <p>This parameter is only configurable for public zone record sets.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • 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)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	300
Value	<p>Email server address</p> <p>You can enter up to 50 different IP addresses, each on a separate line.</p> <p>The format is [priority][mail server host name].</p> <p>Configuration rules:</p> <ul style="list-style-type: none"> • priority: priority for an email server to receive emails. A smaller value indicates a higher priority. • mail server host name: domain name provided by the email service provider 	10 mailserver.example.com.

Parameter	Description	Example Value
Weight	<p>(Optional) Weight for the record set. The value ranges from 0 to 1000, and the default value is 1.</p> <p>This parameter is only configurable for public zone record sets.</p> <p>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.</p>	1
Tag	<p>(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 3-8.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.</p>	example_key1 example_value1
Description	<p>(Optional) Supplementary information about the record set.</p> <p>The description can contain no more than 255 characters.</p>	-

Table 3-8 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =*<>\, / 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =*<>\, / 	example_value1

- Click **OK**.
- Switch back to the **Record Sets** tab.

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

3.2.5 Adding an AAAA Record Set

Scenarios

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

For more information about each type of record sets, see [Record Set Types and Configuration Rules](#).

Prerequisites

You have a web server and obtained an IPv6 address.

Procedure


1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**. The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. Locate the zone and click **Manage Record Sets** in the **Operation** column.
5. Click **Add Record Set**. The **Add Record Set** dialog box is displayed.
6. Configure the parameters based on [Table 3-9](#).

Table 3-9 Parameters for adding an AAAA record set

Parameter	Description	Example Value
Type	Type of the record set. A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone. For details, see Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?	AAAA – Map domains to IPv6 addresses

Parameter	Description	Example Value
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> ● www: The domain name is www.example.com, which is usually used for a website. ● Left blank: The domain name is example.com. 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, which is usually used for email servers. ● *: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com. 	www
Line	<p>Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return.</p> <p>The default value is Default.</p> <p>This parameter is only configurable for public zone record sets.</p> <ul style="list-style-type: none"> ● Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. ● 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 Value
TTL (s)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	300
Value	<p>IPv6 addresses mapped to the domain name.</p> <p>You can enter up to 50 different IP addresses, each on a separate line.</p>	ff03:0db8:85a3:0:0:8a2e:0370:7334
Weight	<p>(Optional) Weight for the record set. The value ranges from 0 to 1000, and the default value is 1.</p> <p>This parameter is only configurable for public zone record sets.</p> <p>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.</p>	1
Tag	<p>(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 3-10.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.</p>	example_key1 example_value1
Description	<p>(Optional) Supplementary information about the record set.</p> <p>The description can contain no more than 255 characters.</p>	-

Table 3-10 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each resource.• Can contain no more than 36 characters.• Cannot start or end with a space nor contain special characters =*<>\\, /	example_key1
Value	<ul style="list-style-type: none">• Cannot be left blank.• Can contain no more than 43 characters.• Cannot start or end with a space nor contain special characters =*<>\\, /	example_value 1

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

3.2.6 Adding a TXT Record Set

Scenarios

A TXT record set provides description for a domain name. 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.

For more information about each type of record sets, see [Record Set Types and Configuration Rules](#).

Procedure


1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**.
The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. Locate the zone and click **Manage Record Sets** in the **Operation** column.
5. Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.
6. Configure the parameters based on [Table 3-11](#).

Table 3-11 Parameters for adding a TXT record set

Parameter	Description	Example Value
Type	<p>Type of the record set</p> <p>A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone.</p> <p>For details, see Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?</p>	TXT – Specify text records
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> • www: The domain name is www.example.com, which is usually used for a website. • Left blank: The domain name is example.com. 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, which is usually used for email servers. • *: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com. 	Left blank

Parameter	Description	Example Value
Line	<p>Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return.</p> <p>The default value is Default.</p> <p>This parameter is only configurable for public zone record sets.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • 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)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	300

Parameter	Description	Example Value
Value	<p>Text content</p> <p>Configuration rules:</p> <ul style="list-style-type: none"> 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. <p>A value must not exceed 4096 characters.</p> <ul style="list-style-type: none"> The value cannot be left blank. The text cannot contain a backslash (\). 	<ul style="list-style-type: none"> 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.
Weight	<p>(Optional) Weight for the record set. The value ranges from 0 to 1000, and the default value is 1.</p> <p>This parameter is only configurable for public zone record sets.</p> <p>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.</p>	1

Parameter	Description	Example Value
Tag	<p>(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 3-12.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.</p>	example_key1 example_value1
Description	<p>(Optional) Supplementary information about the record set.</p> <p>The description can contain no more than 255 characters.</p>	-

Table 3-12 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =* <> \, / 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =* <> \, / 	example_value1

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

Related Operations

For more information about TXT record sets, see [Reclaiming a Public Zone](#).

3.2.7 Adding an SRV Record Set

Scenarios

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

For more information about each type of record sets, see [Record Set Types and Configuration Rules](#).

Procedure


1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**.
The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. Locate the zone and click **Manage Record Sets** in the **Operation** column.
5. Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.
6. Configure the parameters based on [Table 3-13](#).

Table 3-13 Parameters for adding an SRV record set

Parameter	Description	Example Value
Type	Type of the record set A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone. For details, see Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?	SRV – Record servers providing specific services
Name	Service (for example, FTP, SSH, or SIP) provided over the specified protocol (for example, TCP or UDP) on a host The format is <i>_Service name._Protocol</i> .	_ftp._tcp _ftp._tcp indicates that the host provides the FTP service over TCP.

Parameter	Description	Example Value
Line	<p>Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return. The default value is Default.</p> <p>This parameter is only configurable for public zone record sets.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • 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)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	300
Value	<p>Server address</p> <p>You can enter up to 50 different IP addresses, each on a separate line.</p> <p>The value format is [priority] [weight] [port number] [server address].</p> <p>Configuration rules:</p> <ul style="list-style-type: none"> • The priority, weight, and port number range from 0 to 65535. • A smaller value indicates a higher priority. • A larger value indicates a larger weight. • The server address is the domain name of the target server. Ensure that the domain name can be resolved. <p>NOTE If the record set values have the same priority, requests to the domain name will be routed based on weights.</p>	2 1 2355 example_server.test.com

Parameter	Description	Example Value
Weight	<p>(Optional) Weight for the record set. The value ranges from 0 to 1000, and the default value is 1.</p> <p>This parameter is only configurable for public zone record sets.</p> <p>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.</p>	1
Tag	<p>(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 3-14.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.</p>	example_key1 example_value1
Description	<p>(Optional) Supplementary information about the record set.</p> <p>The description can contain no more than 255 characters.</p>	-

Table 3-14 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =*<>\, / 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =*<>\, / 	example_value1

- Click **OK**.
- Switch back to the **Record Sets** tab.

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

3.2.8 Adding an NS Record Set

Scenarios

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

For more information about each type of record sets, see [Record Set Types and Configuration Rules](#).

Constraints

- You can create NS record sets only in public zones.
- After a public zone is created, an NS record set is automatically created for this zone and cannot be deleted. You can add NS record sets only in the following scenarios:
 - The **Name** parameter is not left blank. This means that you can add NS record sets for subdomains of a domain name.
 - The value of the **Line** parameter is not set to **Default**. This means that you can add NS record sets for the domain name with other resolution lines.

Procedure

1. Go to the [Public Zones](#) page.
2. Locate the zone and click **Manage Record Sets** in the **Operation** column.
3. Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.
4. Configure the parameters based on [Table 3-15](#).

Table 3-15 Parameters for adding an NS record set

Parameter	Description	Example Value
Type	Type of the record set A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone. For details, see Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?	NS – Delegate subdomains to other name servers

Parameter	Description	Example Value
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> • www: The domain name is <code>www.example.com</code>, which is usually used for a website. • Left blank: The domain name is <code>example.com</code>. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • abc: The domain name is <code>abc.example.com</code>, a subdomain of <code>example.com</code>. • mail: The domain name is <code>mail.example.com</code>, which is usually used for email servers. • *: The domain name is <code>*.example.com</code>, which is a wildcard domain name, indicating all subdomains of <code>example.com</code>. 	abc
Line	<p>Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return.</p> <p>The default value is Default.</p> <p>This parameter is only configurable for public zone record sets.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • 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)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	300

Parameter	Description	Example Value
Value	DNS server address You can enter up to 50 different IP addresses, each on a separate line.	ns1.example.net ns2.example.net
Weight	(Optional) Weight for the record set. The value ranges from 0 to 1000 , and the default value is 1 . This parameter is only configurable for public zone record sets. 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	(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set. For details about tag key and value requirements, see Table 3-16 . NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set. The description can contain no more than 255 characters.	-

Table 3-16 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =*<>\\, / 	example_key1

Parameter	Requirements	Example Value
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =*<>\\, / 	example_value 1

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

3.2.9 Adding a CAA Record Set

Scenarios

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

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

For more information about each type of record sets, see [Record Set Types and Configuration Rules](#).

Constraints

CAA record sets can be added only to public zones.

Procedure

- Go to the [Public Zones](#) page.
- Locate the zone and click **Manage Record Sets** in the **Operation** column.
- Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.
- Configure the parameters based on [Table 3-17](#).

Table 3-17 Parameters for adding a CAA record set

Parameter	Description	Example Value
Type	<p>Type of the record set</p> <p>A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone.</p> <p>For details, see Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?</p>	CAA – Grant certificate issuing permissions to CAs

Parameter	Description	Example Value
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> • www: The domain name is <code>www.example.com</code>, which is usually used for a website. • Left blank: The domain name is <code>example.com</code>. To use an at sign (@) as the domain name prefix, just leave this parameter blank. • abc: The domain name is <code>abc.example.com</code>, a subdomain of <code>example.com</code>. • mail: The domain name is <code>mail.example.com</code>, which is usually used for email servers. • *: The domain name is <code>*.example.com</code>, which is a wildcard domain name, indicating all subdomains of <code>example.com</code>. 	Left blank
Line	<p>Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return.</p> <p>The default value is Default.</p> <p>This parameter is only configurable for public zone record sets.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • 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)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	300

Parameter	Description	Example Value
Value	<p>CA to be authorized to issue certificates for a domain name or its subdomains</p> <p>You can enter up to 50 different IP addresses, each on a separate line.</p> <p>The format is [flag] [tag] [value].</p> <p>Configuration rules:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> - 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 no more than 255 characters. Only letters, digits, spaces, and special characters -#*?&_~=:;.@+^/!% are allowed. 	<p>0 issue "ca.abc.com"</p> <p>0 issuewild "ca.def.com"</p> <p>0 iodef "mailto:admin@domain.com"</p> <p>0 iodef "http://domain.com/log/"</p>
Weight	<p>(Optional) Weight for the record set. The value ranges from 0 to 1000, and the default value is 1.</p> <p>This parameter is only configurable for public zone record sets.</p> <p>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.</p>	1

Parameter	Description	Example Value
Tag	<p>(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 3-18.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.</p>	example_key1 example_value1
Description	<p>(Optional) Supplementary information about the record set.</p> <p>The description can contain no more than 255 characters.</p>	-

Table 3-18 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =*<> \, / 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =*<> \, / 	example_value1

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

Related Operations

For more information about CAA record sets, see [Setting CAA Record Sets to Prevent Unauthorized HTTPS Certificate Issuing](#).

3.2.10 Adding a PTR Record Set

Scenarios

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

For more information about each type of record sets, see [Record Set Types and Configuration Rules](#).

Constraints

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

For details about how to create a PTR record for a public domain name, see [Creating a PTR Record](#).

Procedure


- Go to the [Private Zones](#) page.
- Click  in the upper left corner and select the desired region and project.
- Locate the zone and click **Manage Record Sets** in the **Operation** column.
- Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.
- Configure the parameters based on [Table 3-19](#).

Table 3-19 Parameters for adding a PTR record set

Parameter	Description	Example Value
Type	Type of the record set A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone. For details, see Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?	PTR – Map IP addresses to domains

Parameter	Description	Example Value
Name	Name of the PTR record set	10.1.168 For example, if the IP address is 192.168.1.10, the domain name in the PTR record is 10.1.168.192.in-addr.arpa . <ul style="list-style-type: none"> • If the domain name is 192.in-addr.arpa, enter 10.1.168. • If the domain name is 1.168.192.in-addr.arpa, enter 10.
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from 1 to 2147483647 , and the default value is 300 . If your service address changes frequently, set TTL to a smaller value. Learn more about TTL .	300
Value	Private domain name mapped to the private IP address. You can enter only one domain name.	host.example.com.
Tag	(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set. For details about tag key and value requirements, see Table 3-20 . NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set. The description can contain no more than 255 characters.	-

Table 3-20 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each resource.• Can contain no more than 36 characters.• Cannot start or end with a space nor contain special characters =*<>\, /	example_key1
Value	<ul style="list-style-type: none">• Cannot be left blank.• Can contain no more than 43 characters.• Cannot start or end with a space nor contain special characters =*<>\, /	example_value 1

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

Related Operations

For more information, see [How Can I Configure a PTR Record to Map the IP Address of an ECS to a Domain Name?](#)

3.3 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.

Huawei Cloud DNS allows you to disable or enable public domain names, private domain names, and record sets configured for public and private domain names.

This topic uses a public zone as an example to describe how you can enable or disable the record sets configured for a public domain name.

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**.

3.4 Managing Record Sets

Scenarios

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


Modifying a Record Set

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

 **NOTE**

- 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 **DNS console**.
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**.
The zone list is displayed.


3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. In the zone list, locate the zone and click the domain name.
The **Record Sets** tab is displayed.
5. Locate the record set you want to modify and click **Modify** in the **Operation** column.
The **Modify Record Set** dialog box is displayed.
6. Modify the parameters.
You can change only the TTL, value, and description of a record set.
7. Click **OK**.

Deleting a Record Set

NOTE

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

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

1. Go to the [DNS console](#).
2. On the **Overview** page, click **Public Zones** or **Private Zones** under **My Resources**.
The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. In the zone list, locate the zone and click the domain name.
The **Record Sets** tab is displayed.
5. Locate the record set you want to delete and click **Delete** in the **Operation** column.
6. In the displayed dialog box, confirm the record set to be deleted.
Enter **DELETE** and click **OK**.


Deleting Record Sets

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


NOTE

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

1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**.
The zone list is displayed.

3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. Select the record sets you want to delete and click **Delete**.
5. In the displayed dialog box, confirm the record sets to be deleted.
Enter **DELETE** and click **OK**.

Viewing Details About a Record Set

1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**.
The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. In the zone list, locate the zone and click the domain name.
The **Record Sets** tab is displayed.
5. Locate the record set view the details.

3.5 Configuring a Wildcard DNS Record Set

Scenarios

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

NOTE

Exact match has a higher priority than fuzzy match.

Constraints

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

Procedure


1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**.
The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. Click the name of the zone to which you want to add a wildcard DNS record set.
5. Click **Add Record Set**.
6. Configure the parameters based on [Table 3-21](#).

Table 3-21 Parameters for adding a wildcard DNS record set

Parameter	Description	Example Value
Name	Public (or private) domain name Enter an asterisk (*) as the leftmost label of the domain name, for example, *.example.com . NOTE Only the leftmost asterisk is considered as a wildcard character. Other asterisks in the domain name are common text characters.	*.abc
Type	Record set type Wildcard DNS resolution does not support NS and SOA record sets.	A – Map domains to IPv4 addresses
Line	The default value is Default . This parameter is only configurable for public zone record sets. <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • 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)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from 1 to 2147483647 , and the default value is 300 . If your service address changes frequently, set TTL to a smaller value. Learn more about TTL .	300
Value	Record set value	Take an A record set for example, Value is set to IPv4 addresses mapped to the domain name. Example: 192.168.12.2 192.168.12.3

Parameter	Description	Example Value
Weight	(Optional) Weight for the record set. The value ranges from 0 to 1000 , and the default value is 1 . This parameter is only configurable for public zone record sets. 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	(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set. For details about tag key and value requirements, see Table 3-22 .	example_key1 example_value1
Description	(Optional) Supplementary information about the record set. The description can contain no more than 255 characters.	This is a wildcard DNS record set.

Table 3-22 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =*<>\\, / 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =*<>\\, / 	example_value 1

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

How Do I Check Whether a Record Set Has Taken Effect?

3.6 Searching for Record Sets

Scenarios

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

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

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

Procedure

1. Go to the [DNS console](#).
2. On the **Dashboard** page, click **Record Sets**.
The record set list is displayed.
3. Click **Private Zone Record Sets**.
4. Set search criteria to search for record sets.
The following search criteria are available:
 - **Domain Name:** Search for record sets by domain name.
 - **Value:** Search for record sets based on their values.
 - **ID:** Search for record sets based on their IDs.
 - **Status:** Search for record sets in a specified state.
 - **Type:** Search for record sets of a specified type.
 - **Tag:** Search for record sets using predefined tags.
5. Click **Modify** or **Delete** to perform desired record set operations.

3.7 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. This feature is available for both public and private zones.


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

NOTE

Before importing record sets, you need to have created public or private zones on the DNS console. For details, see [Creating a Public Zone](#) or [Creating a Private Zone](#).

This section uses example.com as an example to describe how to import record sets.

Procedure

1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**.
The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. In the zone list, click the domain name **example.com** (an example domain name used in this topic).
5. Click **Export and Import**.
 - a. Click **Download template**.
 - b. Enter your record sets in the template as required.

NOTE

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

6. Click **Import Record Set** and select the record set file to import.
After the import is complete, you can check whether record sets are successfully imported or not.
 - **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.

3.8 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. This feature is available for both public and private zones.

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

example.com is used as an example to describe how you can export all its record sets.

Procedure

1. Go to the [DNS console](#).
2. In the navigation pane on the left, choose **Public Zones** or **Private Zones**.
The zone list is displayed.
3. (Optional) If you have selected **Private Zones**, click  on the upper left corner to select the region and project.
4. In the zone list, click the domain name **example.com**.
5. Click the **Export and Import** tab.
6. Click **Export Record Set**.

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 (a public zone record set used as an example): 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.

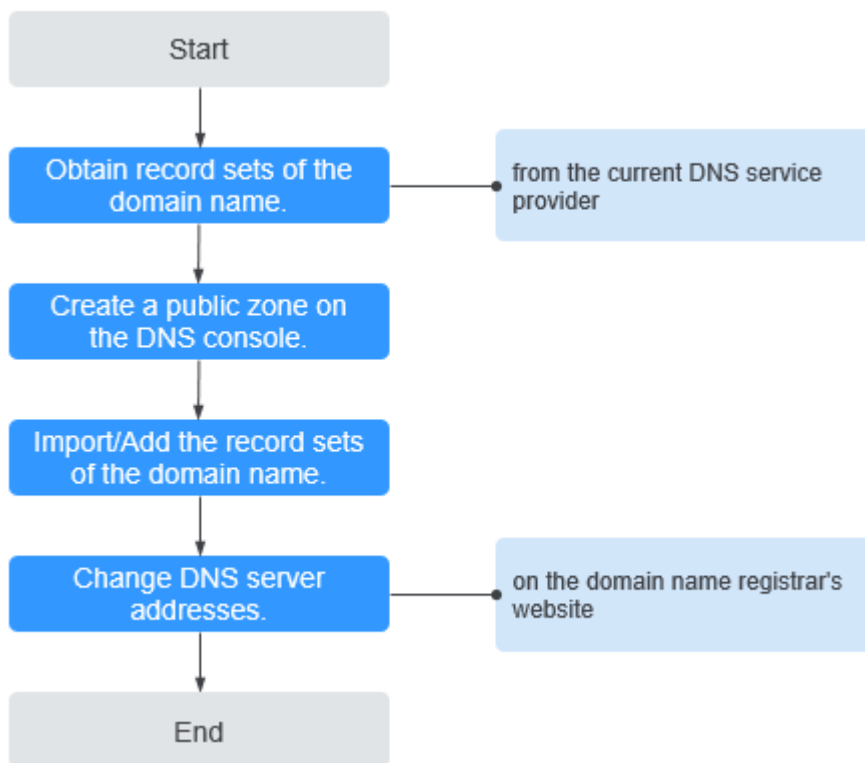
3.9 Migrating to Huawei Cloud DNS for Domain Name Resolution

Scenarios

If you have registered a domain name that is being used on the Internet, you can change the current DNS service provider to Huawei Cloud DNS for domain name resolution.

Process

[Figure 3-2](#) shows the process for changing the DNS service provider of a domain name to Huawei Cloud DNS.

Figure 3-2 Process for changing the DNS service provider to Huawei Cloud DNS

Obtaining DNS Record Sets

Before you use Huawei Cloud DNS for domain name resolution, migrate all its record sets from the current DNS service provider. It is recommended that you export all record sets at a time if this function is supported by the current DNS service provider. For details about how to migrate the record sets, see the documentation of the DNS service provider.

Creating a Public Zone

On the Huawei Cloud DNS console, create a public zone for the domain name.

For details, see [Creating a Public Zone](#).

Adding Record Sets

On the Huawei Cloud DNS console, add record sets to the created public zone. You can import all record sets obtained from the original DNS service provider.

For details, see [Importing Record Sets](#).

For details, see [How Do I Check Whether Record Sets Have Taken Effect?](#)

Changing DNS Servers for the Domain Name

1. Change the DNS servers for the domain name in the system of the original DNS service provider. For details, see the operation guide on the official website of the DNS service provider.

The following are Huawei Cloud DNS server addresses:

- ns1.huaweicloud-dns.com: DNS server for regions in the Chinese mainland
- ns1.huaweicloud-dns.cn: DNS server for regions in the Chinese mainland
- ns1.huaweicloud-dns.net: DNS server for countries or regions outside the Chinese mainland
- ns1.huaweicloud-dns.org: DNS server for countries or regions outside the Chinese mainland

For more information about the DNS servers, see [What Are Huawei Cloud DNS Servers?](#)

2. Wait for the change to take effect.

Generally, the change to DNS servers is quickly synchronized to top-level DNS servers and then rapidly applied on the Internet. However, some DNS service providers set the TTL value in the NS record set to 48 hours. If the NS record set is cached by a local DNS server, the change will take effect in 48 hours.

Do not delete original record sets until the change takes effect. Your services will continue to be served by the old DNS server before the new DNS server is being used.

4 PTR Records

4.1 PTR Record Overview

Reverse resolution means to obtain a domain name based on an IP address. This is typically used to affirm the credibility of email servers.

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

Table 4-1 PTR record description

Operation	Scenario	Constraints
Creating a PTR Record	Create PTR records for cloud resources such as ECS.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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 3 working days. In case of urgency, [submit a service ticket](#). We will contact CNNIC and APNIC to speed up the process.

The 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**.

Figure 4-1 Creating a PTR record

Create PTR Record
✕

EIP [View EIP](#)

Domain Name [Delete](#)
[Add](#)
Maximum domain names that can be added: 10 Enter a domain name, for example, example.com.

TTL (s)

Tag It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#)
To add a tag, enter a tag key and a tag value below.

You can add 20 tags more tags.

Description
0/255 ↗

4. Configure the parameters based on [Table 4-2](#).

Table 4-2 Parameters for creating a PTR record

Parameter	Description	Example Value
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

Parameter	Description	Example Value
Tag	<p>(Optional) Identifier of the PTR record.</p> <p>Each tag contains a key and a value. You can add up to 20 tags to a PTR record.</p> <p>For details about tag key and value requirements, see Table 4-3.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your PTR records based on the tag policies. If you add a tag that does not comply with the tag policies, PTR records may fail to be created. Contact the administrator to learn more about tag policies.</p>	<p>example_key1 example_value1</p>
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 Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =*<>\\,/ 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =*<>\\,/ 	example_value1

- 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.

- In the DOS window of your local PC that has been connected to the Internet, check whether the PTR record takes effect.
 - Press **Win+R** to open the **Run** dialog box, enter **cmd**, and press **Enter**.
 - 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.

Exporting PTR Records

You can export all or selected PTR records to an XLSX file.


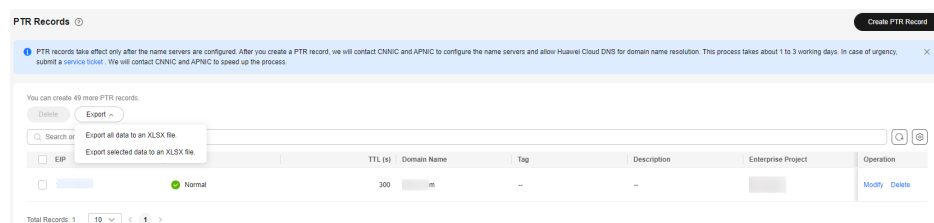
1. Go to the [PTR Records](#) page.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper part of the PTR record list, click **Export**.
4. Select the PTR records to be exported:
 - All PTR records
 - Selected PTR records

Figure 4-2 Exporting PTR records



5 Intelligent Resolution

5.1 Intelligent Resolution Overview

What Is DNS Resolver?

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, the DNS service allows you to define 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 5-1 describes the application scenarios of DNS Resolver.

Table 5-1 Application scenarios of DNS Resolver

Operation	Scenario	Constraints
Configuring ISP Lines for Record Sets	Configure ISP lines to distinguish visitors by carrier.	Resolution lines can be configured only for public zones.
Configuring Region Lines for Record Sets	Configure region lines to distinguish visitors by geographical location.	Resolution lines can be configured only for public zones.

Operation	Scenario	Constraints
Configuring Custom Lines	Configure custom lines to distinguish visitors by IP address range.	Resolution lines can be configured only for public zones.
Configuring Weighted Routing	Configure weight-based resolution for load balancing based on the proportion of requests to each record set.	Resolution lines can be configured only for public zones.

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.

NOTE

ISP lines can be configured only for public zones.

If a resolution line becomes faulty, you cannot switch to another resolution line.

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**.

ISP Lines

ISP lines are categorized by telecom carriers in China.

Table 5-2 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

Level 1	Level 2	Level 3
	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 Tibet
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.
The **Record Sets** tab is displayed.
3. Click **Add Record Set**.
4. Add two A record sets for example.com. Configure the parameters based on [Table 5-3](#).

Table 5-3 Parameters for adding an A record set

Parameter	Description	Line 1	Line 2
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> • www: The domain name is www.example.com, which is usually used for a website. • Left blank: The domain name is example.com. 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, which is usually used for email servers. • *: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com. 	www	www
Type	Type of the record set.	A – Map domains to IPv4 addresses	A – Map domains to IPv4 addresses

Parameter	Description	Line 1	Line 2
Line	<p>Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return.</p> <p>The default value is Default.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • ISP: returns the resolution result based on visitors' carrier networks. • Region: returns the resolution result based on end users' geographical locations. For details, see Configuring Region Lines. 	Default	ISP_China Telecom
TTL (s)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	Default value: 300	Default value: 300
Value	<p>IPv4 addresses mapped to the domain name.</p> <p>Enter each IPv4 address on a separate line.</p>	1.1.1.1	2.2.2.2

Parameter	Description	Line 1	Line 2
Weight	<p>(Optional) Weight for the record set. The value ranges from 0 to 1000, and the default value is 1.</p> <p>This parameter is only configurable for public zone record sets.</p> <p>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.</p>	1	1
Tag	<p>(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 5-4.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.</p>	example_key 1 example_val ue1	example_ke y1 example_val ue1
Description	<p>(Optional) Supplementary information about the record set.</p> <p>The description can contain no more than 255 characters.</p>	-	-

Table 5-4 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =* <> \, / 	example_key1

Parameter	Requirements	Example Value
Value	<ul style="list-style-type: none">• Cannot be left blank.• Can contain no more than 43 characters.• Cannot start or end with a space nor contain special characters =*<>\\, /	example_value 1

5. Click **OK**.

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 5-5](#).

Table 5-5 Region lines

Level 1	Level 2 (Country/Region)	Level 3 (Province)
Asia Pacific	All regions, Taiwan (China), Hong Kong (China), Macao (China), Japan, South Korea, India, Türkiye, Indonesia, Vietnam, Singapore, Thailand, Malaysia, Bangladesh, UAE, Armenia, Azerbaijan, Bahrain, Brunei, Bhutan, Christmas Island, Georgia, Iraq, Jordan, Kyrgyzstan, Cambodia, Kuwait, Kazakhstan, Lebanon, Sri Lanka, Myanmar, Mongolia, Maldives, Nepal, Oman, Philippines, Pakistan, Palestine, Qatar, Saudi Arabia, Tajikistan, Timor-Leste, Turkmenistan, Uzbekistan, Yemen, Cyprus, Israel, American Samoa, Cook Islands, Federated States of Micronesia, Guam, Kiribati, Marshall Islands, Northern Mariana Islands, New Caledonia, Norfolk Island, Nauru, French Polynesia, Papua New Guinea, Palau, Solomon Islands, Tokelau Islands, Tonga, Tuvalu, Vanuatu, Samoa, Afghanistan, Laos, Iran, and Syria	Default
Europe	All regions, United Kingdom, Germany, France, Italy, Russia, Spain, Ukraine, the Netherlands, Sweden, Poland, British Indian Ocean Territory, Belarus, Andorra, Albania, Austria, Aland Islands, Belgium, Bulgaria, Switzerland, Czech Republic, Denmark, Estonia, Finland, Faroe Islands, Guernsey, Gibraltar, Greece, Croatia, Hungary, Ireland, Isle of Man, Iceland, Jersey, Liechtenstein, Lithuania, Luxembourg, Latvia, Monaco, Moldova, Montenegro, North Macedonia, Malta, Norway, Portugal, Romania, Serbia, Slovenia, Slovakia, San Marino, Vatican, Kosovo, Svalbard and Jan Mayen, and Bonaire, Sint Eustatius and Saba	Default
North America	All regions, United States, Canada, Mexico, Antigua and Barbuda, Barbados, Bahamas, Belize, Costa Rica, the Commonwealth of Dominica, the Dominican Republic, Grenada, Guatemala, Honduras, Haiti, Jamaica, Saint Kitts and Nevis, Cayman Islands, Saint Lucia, Nicaragua, Panama, Puerto Rico, El Salvador, Turks and Caicos Islands, Trinidad and Tobago, British Virgin Islands, U.S. Virgin Islands, Saint Vincent and the Grenadines, Saint Martin (French part), Saint Pierre and Miquelon, Cuba, Greenland, Martinique, and Sint Maarten (Dutch part)	Default
South America	All regions, Brazil, Argentina, Anguilla, Aruba, Saint Barthélemy, Bermuda, Guadeloupe, Montserrat, Bolivia, Chile, Colombia, Curaçao, Ecuador, French Guiana, Guyana, Peru, Paraguay, Suriname, Uruguay, and Venezuela	Default

Level 1	Level 2 (Country/Region)	Level 3 (Province)
Africa	All regions, South Africa, Egypt, Angola, Burkina Faso, Burundi, Benin, Botswana, Congo-Kinshasa, Central African Republic, the Republic of Congo, Côte d'Ivoire, Cameroon, Cape Verde, Djibouti, Algeria, Eritrea, Ethiopia, Gabon, Ghana, Gambia, Guinea, Equatorial Guinea, Guinea-Bissau, Kenya, Comoros, Liberia, Lesotho, Libya, Morocco, Madagascar, Mali, Mauritania, Mauritius, Malawi, Mozambique, Niger, Nigeria, Reunion, Rwanda, Seychelles, Sierra Leone, Senegal, Somalia, South Sudan, Sao Tome and Principe, Eswatini, Chad, Togo, Tunisia, Tanzania, Uganda, Mayotte, Zambia, Zimbabwe, Namibia, and Sudan	Default
Oceania	All regions, Australia, New Zealand, Fiji, Wallis and Futuna, and Niue	Default
Antarctica	All regions	Default
Chinese mainland	All regions	-
	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

Level 1	Level 2 (Country/Region)	Level 3 (Province)
	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 Tibet
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.
The **Record Sets** tab is displayed.
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 5-6**.

Table 5-6 Parameters for adding an A record set

Parameter	Description	Line 1	Line 2
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> • www: The domain name is www.example.com, which is usually used for a website. • Left blank: The domain name is example.com. 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, which is usually used for email servers. • *: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com. 	www	www
Type	Type of each record set.	A – Map domains to IPv4 addresses	A – Map domains to IPv4 addresses

Parameter	Description	Line 1	Line 2
Line	<p>The default value is Default.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • ISP: returns the resolution result based on end users' carrier networks. For details, see Configuring ISP Lines. • Region: returns the resolution result based on visitors' geographical locations. 	Default	Select Region and Asia Pacific > Hong Kong (China) .
TTL (s)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p> <p>Learn more about TTL.</p>	Default value: 300	Default value: 300
Value	<p>IPv4 addresses mapped to the domain name.</p> <p>Enter each IPv4 address on a separate line.</p>	1.1.1.1	3.3.3.3
Weight	<p>(Optional) Weight for the record set. The value ranges from 0 to 1000, and the default value is 1.</p> <p>This parameter is only configurable for public zone record sets.</p> <p>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.</p>	1	1

Parameter	Description	Line 1	Line 2
Tag	<p>(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 5-7.</p> <p>NOTE If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.</p>	example_key1 example_value1	example_key1 example_value1
Description	<p>(Optional) Supplementary information about the record set.</p> <p>The description can contain no more than 255 characters.</p>	-	-

Table 5-7 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =*<> \, / 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =*<> \, / 	example_value1

- Click **OK**.

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 5-8](#).

Table 5-8 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.
The **Record Sets** tab is displayed.
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 5-9](#).

Table 5-9 Parameters for adding an A record set

Parameter	Description	Line 1	Line 2
Name	<p>Prefix of the domain name to be resolved.</p> <p>For example, if the domain name is example.com, the prefix can be as follows:</p> <ul style="list-style-type: none"> • www: The domain name is www.example.com, which is usually used for a website. • Left blank: The domain name is example.com. 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, which is usually used for email servers. • *: The domain name is *.example.com, which is a wildcard domain name, indicating all subdomains of example.com. 	www	www
Type	Type of the record set	A – Map domains to IPv4 addresses	A – Map domains to IPv4 addresses

Parameter	Description	Line 1	Line 2
Line	<p>The default value is Default.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. • 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. • Custom line: returns the resolution result based on specified IP address ranges. 	Resolution Lines_Line1	Resolution Lines_Line2
TTL (s)	<p>Cache duration of the record set on a local DNS server, in seconds.</p> <p>The value ranges from 1 to 2147483647, and the default value is 300.</p> <p>If your service address changes frequently, set TTL to a smaller value.</p>	Default value: 300	Default value: 300
Value	<p>IPv4 addresses mapped to the domain name.</p> <p>Enter each IPv4 address on a separate line.</p>	1.1.1.1	2.2.2.2
Tag	<p>(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 5-10.</p> <p>NOTE</p> <p>If your organization has configured tag policies for the DNS service, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.</p>	example_key1 example_value1	example_key1 example_value1

Parameter	Description	Line 1	Line 2
Description	(Optional) Supplementary information about the record set. The description can contain no more than 255 characters.	-	-

Table 5-10 Tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain no more than 36 characters. Cannot start or end with a space nor contain special characters =*<>\\ / 	example_key1
Value	<ul style="list-style-type: none"> Cannot be left blank. Can contain no more than 43 characters. Cannot start or end with a space nor contain special characters =*<>\\ / 	example_value 1

- Click **OK**.

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 192.168.1.1, 192.168.1.2, and 192.168.1.3.

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

For details, see [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

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

Preparations

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

Table 5-11 Weight setting plans

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

Prerequisites

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

Procedure

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

1. Go to the [Public Zones](#) page.
2. On the **Public Zones** page, click the domain name (**example.com**) of the public zone.
The **Record Sets** tab is displayed.
3. Click **Add Record Set**.
4. Configure the parameters as follows:
 - **Name:** Leave this parameter blank. This is a record set for the domain name, which is example.com.
 - **Type:** Retain the default setting **A – Map domains to IPv4 addresses**.
 - **Line Type:** Select **Default**.
 - **Value:** Set it to **192.168.1.1**, the IP address of a web server.
 - **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 192.168.1.2 and 192.168.1.3, respectively.
Requests will be evenly distributed to the three servers.

6 Resolver

6.1 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.

NOTE

DNS Resolver is now available in CN North-Ulanqab1, CN Southwest-Guiyang1, AP-Bangkok, AP-Singapore, AP-Jakarta, LA-Sao Paulo1, TR-Istanbul, AF-Johannesburg, and ME-Riyadh.

Constraints

- Both inbound and outbound endpoints do not support DNSSEC.
- By default, cloud servers use private DNS for domain name resolution. Do not change private DNS addresses, or forwarding rules will not take effect.

Where to Use

- On-premises servers access a cloud service domain name. For this to work, 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](#).

- Cloud servers access an on-premises domain name. For this to work, you need to create an outbound endpoint, configure endpoint rules, and specify the on-premises domain name to be accessed and the IP addresses of 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](#).

6.2 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 6-1](#).

Figure 6-1 Creating an inbound endpoint

Resolvers / Create Endpoint

Basic Configuration

* Endpoint Type Inbound Outbound

* Endpoint Name
Enter a maximum of 64 characters. Only letters, digits, hyphens (-), underscores (_), and dots (.) are allowed.

Region

* VPC
All inbound DNS requests will be routed from this VPC to DNS servers in other VPCs. You cannot change the VPC after you create an endpoint.

IP Addresses

To improve reliability, you need to specify at least two IP addresses in different AZs. You can optionally add more IP addresses.

<p>IP Address 1</p> <p>* Subnet <input type="text" value="--Select--"/> <small>The subnet must have available IP addresses. Only IPv4 addresses are supported.</small></p> <p>AZ --</p> <p>IP Address <input type="button" value="Automatically assign"/> <input type="button" value="Specify"/></p>	<p>IP Address 2</p> <p>* Subnet <input type="text" value="--Select--"/> <small>The subnet must have available IP addresses. Only IPv4 addresses are supported.</small></p> <p>AZ --</p> <p>IP Address <input type="button" value="Automatically assign"/> <input type="button" value="Specify"/></p>
---	---



 Add IP Address

Table 6-1 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: <ul style="list-style-type: none">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 **OK**.

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**.

6.3 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 6-2](#).

Figure 6-2 Creating an outbound endpoint

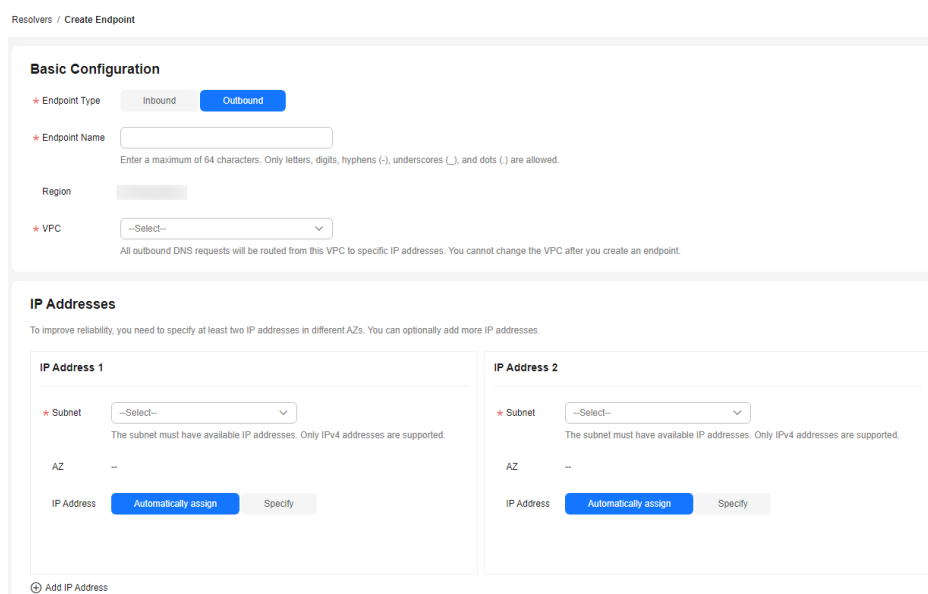


Table 6-2 Parameters for creating an outbound endpoint


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: <ul style="list-style-type: none">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 requests 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 **OK**.


 **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**.

6.4 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 Rule**.
5. Configure the parameters based on [Table 6-3](#).

Figure 6-3 Adding an endpoint rule

Add Endpoint Rule

Basic Information

Name

Domain Name
The domain name cannot be changed after the rule is created.

Type

Outbound Endpoint

Associate VPC

Associate VPC

Region

VPC [View VPC](#)

IP Addresses

IP Address

 Add

Table 6-3 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.


Parameter	Description
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**

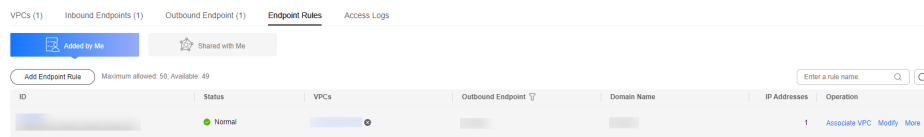
If only one IP address is configured for the endpoint rule, the IP address cannot be deleted.

Deleting an Endpoint Rule

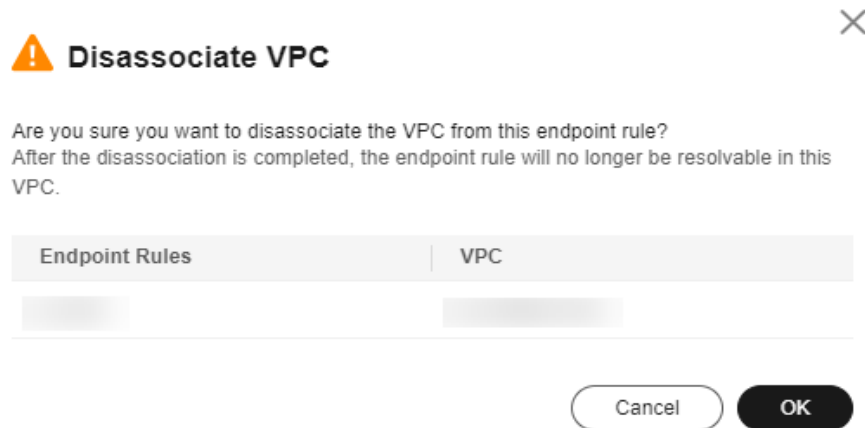
1. Go to the [Resolvers](#) page.
2. Click  in the upper left corner and select the desired region and project.
3. Click the **Endpoint Rules** tab to view the endpoint rule list.
4. Locate the endpoint rule and choose **More > Delete** in the **Operation** column.
5. Confirm the endpoint rule and click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



6.5 Sharing an Endpoint Rule

Overview

You can also share your endpoint rules to other accounts if you are the owner of these rules. Resource owners can select different permissions based on the


principle of least privilege (PoLP) and service requirements, and principals can only access resources within their permissions. This improves resource security. For more information about RAM, see [What Is Resource Access Manager?](#)

If your account is managed by Huawei Cloud Organizations, you can enable sharing with Organizations to share resources more easily. If your account is in an organization, you can share resources either with individual accounts or with all accounts in the organization or in an organization unit (OU) without the need to enumerate each account. For details, see [Enabling Sharing with Organizations](#).

Constraints

- You are the resource owner. Only resource owners can share the resources in their accounts with other accounts. You cannot share endpoint rules that are shared with your account.
- If you share an endpoint rule with your organization or an OU, you must enable sharing with Organizations. For details, see [Enabling Sharing with Organizations](#).
- A principal can accept up to 50 endpoint rules from resource owners.

Creating a Share


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** > **Share** in the **Operation** column.
5. On the **Create Resource Share** page, specify the resource to be shared, configure permissions, and specify users as prompted.

For details, see [Creating a Resource Share](#).

NOTE

After an owner shares an endpoint rule with a principal, the principal needs to accept or reject the sharing within a specified period. For details, see [Responding to a Resource Sharing Invitation](#).

Viewing Share Details

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. Go to the **Shared with Me** tab and view the endpoint rules that are shared with your account.

NOTE

- If you are the owner of a shared endpoint rule, you can view the shared endpoint rule, permissions, and principals on the RAM console. For details, see [Viewing a Resource Share](#).
- If you are a principal of a shared endpoint rule, you can view the shared endpoint rule, permissions, and resource owner on the RAM console. For details, see [Viewing Resources Shared with You](#).

Stopping a Share

- If a share is no longer needed, you can delete it at any time as the owner. Deleting a share does not delete the shared resources. After a share is deleted, the principals will no longer use the shared resources. For details, see [Deleting a Resource Share](#).
- If you are a principal and you do not need to access the shared resources, you can leave the resource share at any time. After you leave a resource share, you lose access to the shared resources.

You can leave a resource share only if the resources were shared with you as an individual Huawei Cloud account and not as part of an organization. You cannot leave a resource share if you were added to it by an account inside your organization and sharing with Organizations is enabled. For details, see [Leaving a Resource Share](#).

Operation Permissions on Shared Endpoint Rules

The owner and principals of shared endpoint rule have different operation permissions on the endpoint rule and associated resources. For details, see [Table 6-4](#).

Table 6-4 Operation permissions on shared endpoint rules and associated resources

Resource	Owner	Principal
Endpoint rule	Has all operation permissions on the shared endpoint rule.	Can only view the VPCs that are associated with the shared endpoint rule, but cannot perform any operations on the VPCs.

Resource and Region Availability

[Table 6-5](#) lists the resources that can be shared and regions where resource sharing is supported.

Table 6-5 Resources that can be shared and regions where resource sharing is supported

Cloud Service	Resource Type	Regions Where Sharing Is Available
DNS	Endpoint rules	CN North-Ulanqab1, CN Southwest-Guiyang1, AP-Bangkok, AP-Singapore, AP-Jakarta, LA-Sao Paulo1, TR-Istanbul, and AF-Johannesburg

Billing

Endpoint rules are free of charge.

7 Permissions Management

7.1 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.

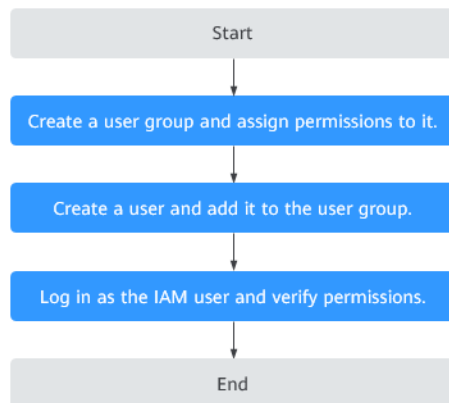
[Figure 7-1](#) shows the process of granting permissions.

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 7-1 Process for granting permissions



1. **Create a user group and assign permissions.**
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. **Create a user and add the user to the user group**
The user group is the one you have created in step 1.
3. **Log in to the management console as the created user.**
Verify that the user only has read permissions for DNS.
 - Choose **Service List > Domain Name Service**. On the DNS console, choose **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.

7.2 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: Defining permissions for multiple services in a policy

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 actions of multiple actions:

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

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

8 Using CTS to Collect DNS Key Operations

8.1 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 8-1](#) and [Table 8-2](#) list the DNS operations that will be recorded by CTS.

NOTE

The DNS service involves resources both at the global and region levels. [Table 8-1](#) lists DNS operations at the global level. Traces of these operations are displayed only in the primary region.

[Table 8-2](#) lists DNS operations at the region level. Traces of these operations are displayed in the regions where the operations are performed.

Table 8-1 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	createPublicRecordSet	A record set is added to a public zone.
Deleting a record set from a public zone	publicRecordSet	deletePublicRecordSet	A record set is deleted from a public zone.
Modifying a record set of a public zone	publicRecordSet	updatePublicRecordSet	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.
Batch disabling or enabling record sets added to a public zone	publicRecordSetStatusBatch	updatePublicRecordSetStatusBatch	Public zone record sets are disabled or enabled in batches.

Table 8-2 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	createPrivateRecordSet	A record set is added to a private zone.
Deleting a record set from a private zone	privateRecordSet	deletePrivateRecordSet	A record set is deleted from a private zone.
Modifying a record set of a private zone	privateRecordSet	updatePrivateRecordSet	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.

Operation	Resource Type	Trace Name	Description
Adding a tag to a private zone	privateZoneTag	createPrivateZone-Tag	A tag is added to a private zone for easier identification.
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.



8.2 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 & Governance > 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.

9 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

LTS is a regional service. You can only enable access logging for the DNS service in the following regions: CN Southwest-Guiyang1, AP-Jakarta, AP-Singapore, AF-Johannesburg, TR-Istanbul, and LA-Sao Paulo1.


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. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click  and choose **Management & Governance > Log Tank Service**.
4. In the navigation pane on the left, choose **Log Management**.
5. Click **Create Log Group**. In the displayed dialog box, enter a name for the log group.
Set **Log Retention Duration** as needed.
6. 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 9-1](#). 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 9-1 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- ac25-4908-8e31-8f f73ad2f57d

Field	Description	Value Description	Example Value
_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. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click  and choose **Management & Governance > Log Tank Service**.
4. In the navigation pane on the left, choose **Log Transfer**.
5. In the upper right corner of the **Log Transfer** page, click **Configure Log Transfer**.

Figure 9-1 Configuring log transfer

Configure Log Transfer

* Log Source Account Current Other

* Enable Transfer

* Transfer Destination OBS DIS

* Log Group Name --Select-- C

* Enterprise Project Name --Select-- C [View Enterprise Projects](#)

* Log Stream Name --Select-- ?

* OBS Bucket --Select-- C [View OBS Bucket](#)

LTS will be authorized to read data from and write data to the selected OBS bucket. When modifying the bucket policy, ensure that LTS has read and write permissions for the bucket to prevent log transfer failures.

Custom Log Transfer Path ?

Log Prefix ?

* Format Raw Log Format

* Log Transfer Interval 3 hours ?

* Time Zone (UTC) Coordinated Universal Time

* Filter by Tag Fields ?

OK Cancel

6. Configure the parameters. For details, see the [Log Tank Service User Guide](#).

10 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?


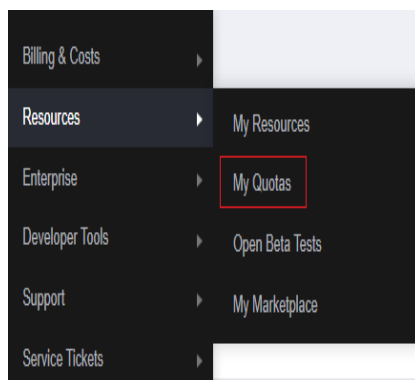
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Service Quota** page is displayed.

Figure 10-1 My Quotas

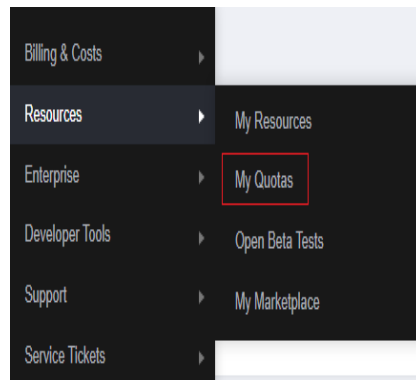


4. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

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 **Service Quota** page is displayed.

Figure 10-2 My Quotas



3. Click **Increase Quota** in the upper right corner of the page.

Figure 10-3 Increasing quota

Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	
	AS configuration	0	
Image Management Service	Image	0	
Cloud Container Engine	Cluster	0	
FunctionGraph	Function	0	
	Code storage(MB)	0	
Elastic Volume Service	Disk	3	
	Disk capacity(GB)	120	
Storage Disaster Recovery Service	Snapshots	4	
	Protection group	0	
Cloud Server Backup Service	Replication pair	0	
	Backup Capacity(GB)	0	
Scalable File Service	Backup	0	
	File system	0	
CDN	File system capacity(GB)	0	
	Domain name	0	
	File URL refreshing	0	
	Director URL refreshing	0	
	URL prewarming	0	
	URL prewarming	0	

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**.