

Domain Name Service

FAQs

Issue 01
Date 2024-05-30



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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.

Contents

1 DNS Overview.....	1
1.1 Will I Be Billed for the DNS Service?.....	1
1.2 How Many Zones, PTR Records, and Record Sets Can I Create?.....	1
1.3 What Are Huawei Cloud DNS Servers?.....	1
1.4 What Are Huawei Cloud Private DNS Server Addresses?.....	4
1.5 What Are the Differences Between Public and Private Domain Names?.....	6
1.6 Does DNS Support IPv6?.....	6
1.7 Does DNS Support Explicit and Implicit URLs?.....	6
1.8 Does DNS Support Dynamic Domain Name Resolution?.....	7
1.9 Does DNS Support Wildcard Entries?.....	7
1.10 What Is TTL?.....	7
1.11 How Many Domain Name Levels Does DNS Support?.....	8
1.12 How Are Zones Queried to Resolve a Domain Name?.....	8
1.13 What Are the Priorities of Resolution Lines?.....	8
1.14 Why Was the Email Address Format Changed in the SOA Record?.....	9
1.15 What Is CAA?.....	9
1.16 Why Should I Set Priority For an MX Record Set?.....	11
1.17 Can DNS Point a Domain Name to a Specific Port?.....	11
2 Invalid Domain Resolution.....	12
2.1 What Can I Do If a Record Set Does Not Take Effect?.....	12
2.2 How Do I Check Whether a Record Set Has Taken Effect?.....	14
2.3 When Will a New Record Set Take Effect?.....	16
2.4 When Will a Modified or Deleted Record Set Take Effect?.....	16
2.5 When Will New DNS Server Addresses Take Effect?.....	16
3 Website Access Failures.....	18
3.1 Why Can't I Access the Website Even Though the Domain Name Has Been Resolved?.....	18
3.2 Why Can't My Website Be Accessed over HTTPS?.....	18
4 Public Zones.....	19
4.1 Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?.....	19
4.2 How Do I Handle the Conflict Between CNAME and MX Record Sets?.....	22
4.3 How Do I Add Record Sets to Subdomains?.....	24

4.4 Which IP Address Is Returned for the Domain Name If There Are Multiple IP Addresses in a Record Set?.....	26
4.5 Can I Modify a Zone?.....	27
4.6 Can DNS Translate a Domain Name to IP Addresses of On-premises Servers or Third-Party Servers?.....	27
4.7 How Can Multiple Domain Names Be Linked to the Same Website?.....	27
4.8 Configuring Weighted Routing.....	28
4.9 Can DNS Resolve a Domain Name that Has Not Been Licensed?.....	31
4.10 Does DNS Support Dynamic Domain Name Resolution?.....	31
4.11 How Do I View and Change the DNS Servers of a Domain Name?.....	31
5 Private Zones.....	33
5.1 Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?.....	33
5.2 How Do I Change Default DNS Servers of an ECS to Huawei Cloud Private DNS Servers?.....	34
5.3 How Can I Access an ECS Using Its Host Name?.....	35
5.4 How Can I Map the Private IP Address of an ECS to a Domain Name?.....	36
5.5 How Can I Use a Private Domain Name to Route Internet Traffic?.....	41
5.6 Can I Use Private Domain Names Across Regions?.....	41
5.7 Do I Need to Register Private Domain Names?.....	42
5.8 Will a Deleted VPC Be Automatically Disassociated from the Private Zone?.....	42
5.9 Are Private DNS Server Addresses the Same for All Users?.....	43
5.10 What Are the Restrictions on Concurrent Private DNS Requests?.....	43
6 Reverse Resolution.....	44
6.1 What Is Reverse Resolution?.....	44
7 Domain Transfer.....	45
7.1 Can I Transfer a Hosted Public Domain Name from One Account to Another Account?.....	45
7.2 How Do I Migrate My Domain from Another DNS Service Provider to Huawei Cloud DNS?.....	45
8 Change History.....	47

1 DNS Overview

1.1 Will I Be Billed for the DNS Service?

DNS is a free service.

1.2 How Many Zones, PTR Records, and Record Sets Can I Create?

The default quotas for an account are 50 public zones, 50 private zones, 50 PTR records, and 500 record sets.

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

1.3 What Are Huawei Cloud DNS Servers?

DNS provides authoritative DNS servers for domain name resolution. The NS record set defines the addresses of authoritative DNS servers for the domain name.

You can refer to this [FAQ](#) for suggestions on and steps of setting DNS servers.

Huawei Cloud DNS Servers

DNS servers are deployed in multiple AZs around the world so that it can respond to queries for domain names at the lowest latency and support anycast in some regions.

The following are Huawei Cloud DNS servers:

- 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

After you [create a public zone](#) on the DNS console, an NS record set is automatically generated for this zone, and its value is the four DNS servers.

Suggestions on DNS Server Setting

Because the outbound bandwidth from the Chinese mainland is limited, network latency increases when end users access a network outside the Chinese mainland.

To reduce network latency, you can follow the suggestions below to set the NS record set for each public zone:

- If your end users are mainly in the Chinese mainland, use ns1.huaweicloud-dns.com and ns1.huaweicloud-dns.cn.
- If your end users are mainly in countries or regions outside the Chinese mainland, use ns1.huaweicloud-dns.net and ns1.huaweicloud-dns.org.
- If your end users are all over the world, use all four DNS servers.

Procedure for Setting DNS Servers

Step 1 Modify an NS record set.

Set the DNS servers by modifying the NS record set on the **Record Sets** tab.

1. Go to the [Public Zones](#) page.
2. In the public zone list, locate the zone for which record sets you want to modify and click the domain name.
3. On the **Record Sets** tab, locate the NS record set that was automatically generated by the DNS service and click **Modify** under **Operation**.

Figure 1-1 Modify Record Set

Modify Record Set

The screenshot shows a 'Modify Record Set' form with the following fields and values:

- Name: [Empty text box]
- Type: NS – Delegate subdomains to other name servers
- Alias: Yes No
- Line: Default
- TTL (s): 172800 (with buttons for 5 min, 1 h, 12 h, 1 day)
- Value: ns1.huaweicloud-dns.com, ns1.huaweicloud-dns.cn, ns1.huaweicloud-dns.net, ns1.huaweicloud-dns.org
- Weight: Enter an integer from 0 to 1,000.
- Description: [Empty text box]

Buttons: Cancel, OK

4. Change the setting of **Value** based on [Suggestions on DNS Server Setting](#).
5. Click **OK**.

Step 2 Change the DNS servers at the domain name registrar.

For details, see [How Do I View and Change the DNS Servers of a Domain Name?](#)

----End

NOTE

The NS record value of some public zones is set to ns1.hwclouds-dns.com and ns1.hwclouds-dns.net. These addresses are used by Huawei Cloud DNS to provide resolution services for users in earlier versions and will be removed soon.

1.4 What Are Huawei Cloud Private DNS Server Addresses?

Private DNS servers are used in VPCs to:

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

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

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

Table 1-1 lists private DNS server addresses provided by the Huawei Cloud DNS in different regions.

NOTE

- Set the DNS server addresses of the VPC subnet where the ECS resides to the private DNS server addresses of each region. For details, see [How Do I Change Default DNS Servers of an ECS to Huawei Cloud Private DNS Servers?](#)
Table 1-1 lists the private DNS server addresses in each region.
- If you set **DNS Server Address** to external DNS server addresses, traffic will be routed to public IP addresses when ECS accesses other cloud services, which may incur additional traffic fees.
- When an ECS accesses a third-party domain name on the Internet, the private DNS server functions as a recursive DNS server, and the authoritative DNS server returns the final resolution result. Whether the resolution result is reliable or optimal depends on uncontrollable factors such as third-party authoritative DNS. It is recommended that ECSs access cloud services using their private domain names.

Table 1-1 Private DNS server addresses

Region	Private DNS Server Address
CN North-Beijing1	100.125.1.250
	100.125.21.250
CN North-Beijing4	100.125.1.250
	100.125.129.250
CN Southwest-Guiyang1	100.125.1.250
	100.125.129.250
CN South-Guangzhou	100.125.1.250
	100.125.136.29
CN East-Shanghai1	100.125.1.250
	100.125.64.250

Region	Private DNS Server Address
CN East-Shanghai2	100.125.17.29
	100.125.135.29
CN South-Guangzhou-InvitationOnly	100.125.0.167
CN-Hong Kong	100.125.1.250
	100.125.3.250
AP-Bangkok	100.125.1.250
	100.125.1.251
AP-Singapore	100.125.1.250
	100.125.128.250
AP-Jakarta	100.125.2.250
	100.125.2.251
AF-Johannesburg	100.125.1.250
	100.125.1.14
TR-Istanbul	100.125.2.250
	100.125.2.251
LA-Santiago	100.125.1.250
	100.125.0.250
LA-Sao Paulo1	100.125.1.22
	100.125.1.90
LA-Mexico City1	100.125.1.22
	100.125.1.90
LA-Mexico City2	100.125.1.250
	100.125.1.242
ME-Riyadh	100.125.250.249
	100.125.250.250

1.5 What Are the Differences Between Public and Private Domain Names?

The most notable difference between public and private domain names is that public domain names are used and must be unique on the Internet, while private domain names are used in VPCs.

To enable a public domain name to be resolved, you need to perform the following steps:

1. Purchase the domain name from a domain name registrar.
2. Create a zone and add records. For details, see [Routing Internet Traffic to a Website](#).

For details about how a public domain name is resolved, see [Public Zone](#).

Private domain names do not need to be registered and are accessible only in VPCs.

For details about how a private domain name is resolved, see [Routing Traffic Within VPCs](#).

1.6 Does DNS Support IPv6?

Yes. DNS can translate domain names to both IPv4 and IPv6 addresses.

To translate a domain name to an IPv4 address, add an A record set. To translate a domain name to an IPv6 address, add an AAAA record set.

If your domain name is example.com, you can add the following record sets.

Table 1-2 Record sets

Domain Name	Type	Value
www.example.com	A	192.168.1.2
www.example.com	AAAA	2407:c080:0:ffff:ffff:fffe:0:1

Huawei Cloud DNS servers (ns1.huaweicloud-dns.com, ns1.huaweicloud-dns.cn, ns1.huaweicloud-dns.net, and ns1.huaweicloud-dns.org) support both IPv4 and IPv6 addresses.

Local DNS servers, either supporting IPv4 or IPv6 or both, can send DNS queries to DNS servers.

1.7 Does DNS Support Explicit and Implicit URLs?

No.

Explicit or implicit URL forwarding is not performed over a standard DNS protocol, but uses 301 or 302 redirection over HTTP. You can resolve the domain name to the IP address of your cloud server, and then configure 301 or 302 redirection for the domain name on your web server, such as Nginx, Apache, and Internet Information Services (IIS).

1.8 Does DNS Support Dynamic Domain Name Resolution?

No. DNS can only translate domain names to fixed IPv4 and IPv6 addresses.

1.9 Does DNS Support Wildcard Entries?

Yes. DNS allows you to configure wildcard entries.

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

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

1.10 What Is TTL?

TTL (time to live) specifies how long records are cached on a local DNS server.

The local DNS server is connected to clients (computers or smartphones) through the Internet. By default, its address is assigned by the broadband carrier. You can also choose a public DNS server, for example, 114.114.114.114 or 8.8.8.8, as your local DNS server.

When receiving requests for a domain name, the local DNS server asks the authoritative DNS server for the required DNS record, and then caches the record for a period of time. During this period, if the local DNS server receives requests for this domain name again, it will not request the record from the authoritative DNS server, but directly returns the cached record.

The time records are cached on the local DNS server is specified by the TTL value. You can set it when adding record sets in public or private zones. For details, see [Managing Record Sets](#).

The effective time of the following operations depends on the TTL value (to accelerate the process, decrease the TTL value):

- [Adding a record set](#)
- [Modifying or deleting a record set](#)
- [Changing DNS server addresses](#)

1.11 How Many Domain Name Levels Does DNS Support?

The DNS service supports two levels of public domain names.

DNS supports the following levels for domain names with the .com suffix:

- Primary domain name, such as example.com
- Subdomain, such as www.example.com

DNS supports the following levels for domain names with the .com.cn suffix:

- Primary domain name, such as example.com.cn
- Subdomain, such as www.example.com.cn

1.12 How Are Zones Queried to Resolve a Domain Name?

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

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

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

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

1.13 What Are the Priorities of Resolution Lines?

DNS supports the following types of resolution lines in addition to default lines:

- ISP lines
- Region lines

For details, see [Intelligent Resolution Line](#).

If you configure multiple resolution lines for a domain name, their priorities comply with the following principles:

- The priorities of different types of resolution lines are as follows:
ISP lines > Region lines > Default lines
- For region lines, the more accurate the range is, the higher the priority is.
The priorities of regions lines are as follows:

Beijing (Province/State) > North China (Region) > Chinese mainland > Global
> Default

1.14 Why Was the Email Address Format Changed in the SOA Record?

When you add a record set, you can enter an email address to receive error information and problem reports of the domain name. However, based on RFC 2142, we strongly recommend that you use **HOSTMASTER@Domain name** as the email address.

Because the at sign (@) has a special meaning in the SOA record set, the system replaces it with a dot (.) and includes a backslash (\) before the dot in the label before the at sign, but emails are still sent to the email address you have specified. For more information, see RFC 1035.

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

1.15 What Is CAA?

Certification Authority Authorization (CAA) is to ensure that HTTPS certificates are issued by authorized certificate authorities (CAs). CAA complies with all IETF RFC 6844 requirements. As of September 8, 2017, all CAs are required to check CAA record sets before they can issue certificates.

CAA Specifications

Domain name owners can create CAA record sets to specify authorized CAs that can issue SSL certificates.

Only authorized CAs can issue SSL certificates for the domain names used by your website. Setting CAA record sets enhances security for your website.

CAs will perform a DNS lookup for CAA record sets when they issue certificates.

- If a CA does not find a CAA record set, the CA can issue a certificate for the domain name.

Other CAs can also issue certificates for this domain name, but these certificates may be insecure, and there will be messages indicating that your website is insecure when end users access your website.

- If a CA finds a CAA record set that authorizes it to issue certificates, the CA will issue a certificate for the domain name.
- If a CA finds a CAA record set that does not authorize it to issue certificates, the CA will not be able to issue SSL certificates for the domain name.

CAA Record Set

A CAA record set consists of a flag byte **[flag]**, a property tag, and a property value **[tag]-[value]**. You can create multiple CAA record sets for a domain name.

Table 1-3 Configuration of CAA record sets

Function	Example CAA Record Set	Description
Configure a CAA record set for one domain name.	0 issue "ca.example.com "	Only the specified CA (ca.example.com) can issue certificates for a particular domain name (domain.com). Requests to issue certificates for the domain name by other CAs will be rejected.
	0 issue ";"	No CA is allowed to issue certificates for the domain name (domain.com).
Enable a CA to report violations to the domain name holder.	0 iodef "mailto:admin@ domain.com"	If a certificate request violates the CAA record set, the CA will notify the domain name holder of the violation.
	0 iodef "http:// domain.com/log /" 0 iodef "https:// domain.com/log /"	Requests to issue certificates by unauthorized CAs will be recorded.
Authorize a CA to issue wildcard certificates.	0 issuewild "ca.example.com "	The authorized CA (ca.example.com) can issue wildcard certificates for the domain name.
Configuration example	0 issue "ca.abc.com" 0 issuewild "ca.def.com" 0 iodef "mailto:admin@ domain.com"	<p>A CAA record set is configured for domain.com.</p> <ul style="list-style-type: none"> • Only CA ca.abc.com can issue certificates of all types. • Only CA ca.def.com can issue wildcard certificates. • Any other CAs are not allowed to issue certificates. • If a violation occurs, the CA sends a notification to admin@domain.com.

Checking Whether a CAA Record Set Has Taken Effect

Use Domain Information Groper (dig) to check whether the CAA record set has taken effect. dig is a network administration command-line tool for querying the Domain Name System. If your OS does not support dig commands, install the dig tool.

Command format: **dig** [*Record set type*] [*Domain name*] **+trace**.

Example command:

dig caa www.example.com +trace

1.16 Why Should I Set Priority For an MX Record Set?

The priority you set when you add an MX record set specifies the sequence that an email server receives emails. A smaller value indicates a higher priority.

- If there is only one MX record set, the priority is not applied.
- If there are multiple MX record sets, the DNS server of the email sender preferentially sends emails to the email server with the highest priority.
If the email server becomes faulty, the DNS server automatically sends emails to the email server with the second highest priority.

For details about how to add MX record sets, see [Managing Record Sets](#).

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

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

2 Invalid Domain Resolution

2.1 What Can I Do If a Record Set Does Not Take Effect?

Symptom

When you ping the domain name, no IP address is returned. There are many causes why a domain name cannot be resolved.

Troubleshooting Method

- The causes here are described in order of how likely they are to occur. Check these causes one by one until you find the cause of the fault.
 - a. **Checking the Status of the Domain Name:** If the domain name has expired or is abnormal, it cannot be resolved.
 - b. **Checking the DNS Servers of the Domain Name:** If non-Huawei Cloud DNS servers are used for the domain name, the domain name cannot be resolved.
 - c. **Checking the Record Set:** If the record set is incorrect, the domain name cannot be resolved.
 - d. **Checking the DNS Server Changes Within 24 Hours:** Local DNS server caches the NS record configured for the domain name. It may take 48 hours to update the NS record.
 - e. **Checking the Authoritative DNS Server:** Run `nslookup` to check whether the record set takes effect on the authoritative DNS server.
 - f. **Submitting a Service Ticket**

Checking the Status of the Domain Name

A domain name is the entry for DNS resolution. You can use DNS for resolution only if the status of your purchased domain name is normal. If the domain name is in the **serverhold** state, for example, the domain name is in arrears, the real name is not authenticated, or the domain name is disputed, the domain name cannot be resolved.

Checking the DNS Servers of the Domain Name

The DNS service provides authoritative DNS servers for domain resolution.

If non-Huawei Cloud DNS servers are used, the domain name cannot be resolved.

Checking the Record Set

1. Log in to the [DNS console](#) and check the zone status.

If the status is **Disabled**, the domain name cannot be resolved.

2. Check whether the record set is correct and its status is **Normal**.

For example, if the subdomain cannot be accessed, a possible cause is that a record set is added for the second-level domain name but no record set is added for `www`.

Checking the DNS Server Changes Within 24 Hours

The changes the DNS servers do not take effect immediately. Domain name registrars usually set the TTL value in the NS record to 48 hours. If the local DNS server caches the NS record of the domain name, the changes will take effect in 48 hours.

Consult the domain name registrars for specific cache duration. Do not delete original record sets until the changes take effect to ensure your service continuity.

Checking the Authoritative DNS Server

Check whether record sets of the domain name have taken effect on the authoritative DNS server:

```
nslookup -qt= [Record set type] [Domain name] [Authoritative DNS server]
```

If the authoritative DNS server is `ns1.huaweicloud-dns.cn` and the domain name is `example.com`, run the following command:

```
nslookup -qt=a example123.com ns1.huaweicloud-dns.cn
```

If a domain name can be resolved by the authoritative DNS server but the IP address is not returned when the domain name is used for access, the local DNS server may be hijacked. Run either command to check whether public DNS resolution has taken effect: **nslookup -qt=***[Record set type]* *[Domain name]* **8.8.8.8** or **nslookup -qt=***[Record set type]* *[Domain name]* **114.114.114.114**

If public DNS resolution takes effect, change the local DNS server to a public DNS server, for example, `8.8.8.8` or `114.114.114.114`.

Submitting a Service Ticket

If the website still cannot be accessed, [create a service ticket](#) for help.

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

When Will a Record Set Take Effect After It Is Added?

A record set takes effect after it is synchronized to the DNS servers.

- If you add a record set, it takes effect immediately after being added.
- If you modify a record set, the effective time will not be later than the TTL value set in the record set before the modification. For example, if the TTL value is 300s, the new record set will take effect within 300s. If there is no cache delay on the local DNS server, the modification takes effect immediately.

If the carrier forcibly sets a longer cache duration for domain name records, the modification to or deletion of the records will be delayed for a maximum of 48 hours. During the modification, ensure that the IP addresses before and after the modification can provide services properly.

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

Run either command to check whether a record set has taken effect:

- `ping [Domain name]`
- `nslookup -qt=[Record set type] [Domain name]`

For details, see the following:

- [Pinging the Domain Name \(Windows and Linux\)](#)
- [Running nslookup \(Windows and Linux\)](#)
 - [A record set](#)
 - [CNAME record set](#)
 - [MX record set](#)
 - [NS record set](#)
 - [Domain name resolution on an authoritative DNS server](#)

Pinging the Domain Name (Windows and Linux)

1. On your local host, click the search icon and enter `cmd` to open the CLI.
2. Run the following command to check whether the record set is taking effect:

```
ping [Domain name]
```

For example, if the domain name is `example.com`, run `ping example.com`.

If the displayed IP address is the same as the IP address configured in the record set, the record set has taken effect.

NOTE

When you run the ping command, the domain name can be pinged does not mean that the record set has taken effect. If the displayed IP address is the same as the configured IP address, the record set is taking effect.

Running nslookup (Windows and Linux)

- **A record set:** maps a domain name to one or more IP addresses
 - a. On your local host, click the search icon and enter **cmd** to open the CLI.
 - b. Run the following command to check whether the record set is taking effect:
nslookup -qt=a [Domain name]
or
nslookup [Domain name]
Example: **nslookup example.com**
If the displayed IP address is the same as the IP address configured in the record set, the record set has taken effect.
- **CNAME record set:** used for scenarios that involve Content Delivery Network (CDN), WAF, and CloudSite
 - a. On your local host, click the search icon and enter **cmd** to open the CLI.
 - b. Run the following command to check whether the record set is taking effect:
nslookup -qt=cname [Domain name]
Example: **nslookup -qt=cname examplesite.com**
If the displayed domain name is the same as that configured in the record set, the record set has taken effect.
- **MX record set:** used for mail servers
 - a. On your local host, click the search icon and enter **cmd** to open the CLI.
 - b. Run the following command to check whether the record set has taken effect:
nslookup -qt=mx [Domain name]
Example: **nslookup -qt=mx example123.com**
If the displayed mailbox address is the same as that configured in the record set, the record set is taking effect.
- **NS record set:** used to specify the DNS servers
 - a. On your local host, click the search icon and enter **cmd** to open the CLI.
 - b. Run the following command to check whether the record sets are taking effect:
nslookup -qt=ns [Domain name]
Example: **nslookup -qt=ns example123.top**
If the displayed DNS servers are the same as those provided by DNS service provider, the record set has taken effect.
- **Domain name resolution on an authoritative DNS server**
 - a. On your local host, click the search icon and enter **cmd** to open the CLI.
 - b. Run the following command to check whether the record set is taking effect:
nslookup -qt= [Record set type] [Domain name] [Authoritative DNS server]
Example: **nslookup -qt=a example123.com ns1.huaweicloud-dns.cn**

The record set configured for example123.com has taken effect on the authoritative DNS server ns1.huaweicloud-dns.cn.

Common Issues

- If the IP address cannot be obtained during the verification, the record set has not taken effect or has been modified. Rectify the fault by referring to [Why Did My Record Set Not Take Effect?](#)
- An expired domain name has been renewed, but the website still cannot be visited.
A possible cause is that the DNS settings are not refreshed. Run **ipconfig / flushdns** to refresh the settings. Alternatively, wait until the DNS settings are updated and try again.
- The ping command has proved that the domain name can be resolved, but the website cannot be visited.
Ensure that the domain name is correctly bound to the ECSs where the website is deployed or the website has been licensed. Refer to the following to address the issue:
[Why Can't I Access the Website Even Though the Domain Name Has Been Resolved Successfully?](#)

2.3 When Will a New Record Set Take Effect?

- A record set takes effect immediately after it is added.
- If you delete a record set and add it again, it will take effect after the TTL set in the deleted record set expires.
If the carrier forcibly sets a longer cache duration for domain name records, the modification to or deletion of the records will be delayed for a maximum of 48 hours. During the modification, ensure that the IP addresses before and after the modification can provide services properly.

2.4 When Will a Modified or Deleted Record Set Take Effect?

A modified or deleted record set takes effect when the cache duration specified by the TTL set in the original record set expires.

If the carrier forcibly sets a longer cache duration for domain name records, the modification to or deletion of the records will be delayed for a maximum of 48 hours. During the modification, ensure that the IP addresses before and after the modification can provide services properly.

2.5 When Will New DNS Server Addresses Take Effect?

Changes to DNS servers can be quickly synchronized to the top-level domain name servers and then rapidly applied on the entire network. However, some domain name registrars set the TTL value for NS records to 48 hours. If the NS records are cached by a local DNS server, the changes would take effect in 48 hours.

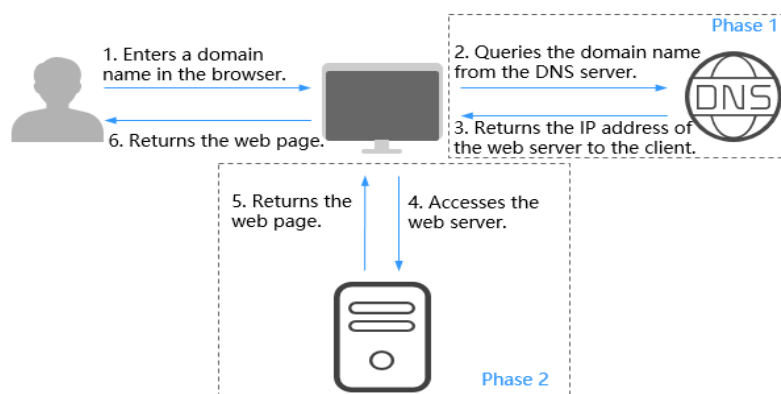
Consult the domain name registrars to learn how long the TTL is. Do not delete original record sets until the changes take effect to ensure your service continuity.

3 Website Access Failures

3.1 Why Can't I Access the Website Even Though the Domain Name Has Been Resolved?

Website access is performed at two necessary phases. [Figure 3-1](#) shows process for accessing a website.

Figure 3-1 How DNS routes Internet traffic to a website



The process consists of two phases:

- Phase 1: The DNS server translates the domain name into the IP address of the web server and returns the IP address to the client.
- Phase 2: The client accesses the web server using the IP address, and the web server returns the desired content.

3.2 Why Can't My Website Be Accessed over HTTPS?

If you want your website to be accessed over HTTPS, deploy an SSL certificate for the website.

4 Public Zones

4.1 Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?

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

[Table 4-1](#) lists the rules.

Table 4-1 Restrictions between record types

	NS	CNAME	A	AAAA	MX	TXT	PTR	SRV	CAA
NS	No limit ^a	Conflict	No limit	No limit	No limit	No limit	No limit	No limit	No limit
CNAME	Conflict ^b	No limit	Conflict	Conflict	Conflict	Conflict	Conflict	Conflict	Conflict
A	No limit	Conflict	No limit	No limit	No limit	No limit	No limit	No limit	No limit
AAAA	No limit	Conflict	No limit	No limit	No limit	No limit	No limit	No limit	No limit
MX	No limit	Conflict	No limit	No limit	No limit	No limit	No limit	No limit	No limit
TXT	No limit	Conflict	No limit	No limit	No limit	No limit	No limit	No limit	No limit
PTR	No limit	Conflict	No limit	No limit	No limit	No limit	No limit	No limit	No limit

SRV	No limit	Conflict	No limit	No limit	No limit	No limit	No limit	No limit	No limit
CAA	No limit	Conflict	No limit	No limit	No limit	No limit	No limit	No limit	No limit
<p>a: NS record sets cannot be added for second-level domain names. There is no such restriction on subdomains.</p> <p>b: For second-level domain names, CNAME and NS record sets can coexist. For subdomains, CNAME record sets conflict with NS record sets.</p>									

The rules are as follows:

- **Conflict:** The two types of record sets cannot have the same resolution line.
- **No limit:** The two types of record sets can coexist.

If the message is displayed, perform the following operations:

- Delete the existing record set that conflicts with the record set that you want to add, and then add the record set back.

 **NOTE**

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

- Set a different name for the record set.
- Select a different line type.

The following are two examples how you can solve common record set conflicts.

Conflicts when Adding an NS Record Set

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

In [Table 4-1](#), NS record sets cannot be added to example.com in the same resolution line.

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

- Method 1: Add an NS record set for a subdomain of example.com.
In the following figure, an NS record set is added for 123.example.com, and the value of the record set is **ns.example.com**.

Figure 4-1 Adding an NS record set

Add Record Set [Close]

Name: [Help]

* Type: [Dropdown]

* Line: [Dropdown] [Help]

* TTL (s): [Help]

* Value: [Help]

Weight: [Help]

More Settings:

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

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

Figure 4-2 Adding an NS record set with an ISP line

Add Record Set [Close]

Name: [Help]

* Type: [Dropdown]

* Line: [Dropdown] [Help]

* TTL (s): [Help]

* Value: [Help]

Weight: [Help]

More Settings:

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

To configure a new DNS server address for a domain name, modify the value of the NS record set added to the hosted zone. For more information, see [What Are Huawei Cloud DNS Servers?](#)

Conflicts when Adding a CNAME Record Set (Pointing to an Email Server)

If you have hosted domain name example.com on the DNS service, add MX, TXT, or CNAME record sets to example.com.

In [Table 4-1](#), if the record set names are the same, the CNAME record set conflicts with MX and TXT record sets with the same resolution line. In this case, you can add a CNAME record set with a different name.

For detailed operations, see [Table 4-2](#).

Table 4-2 Email resolution records

Record Set Type	Name	Value	Description
MX	-	5 mx01.mailserver.com 10 mx02.mailserver.com	Email server address, which is obtained from the email service provider
TXT	-	"v=spf1 include:spf.mailserver.com -all"	SPF records used to prevent spam
CNAME	mail	mailserver.com	Use domain name mail.example.com to log in to the mailbox.
CNAME	smtp	smtp.mailserver.com	Use smtp.example.com as the alias of smtp.mailserver.com.
CNAME	imap	imap.mailserver.com	Use imap.example.com as the alias of imap.mailserver.com.
CNAME	pop	pop.mailserver.com	Use pop.example.com as the alias of pop.mailserver.com.

4.2 How Do I Handle the Conflict Between CNAME and MX Record Sets?

Background

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

For access acceleration or secure purposes, cloud services such as CDN, WAF, and OBS are configured for the website. In this case, A record sets cannot be

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

If this happens, refer to this FAQ to solve the problem. Domain name example.net is used as an example here.

(Recommended) Universal Solution

Accessing a website

1. Add an A record for mapping example.net to the IP address of the website. For details, see [Adding an A Record Set](#).
2. Add a CNAME record set for mapping www.example.net to the domain name of the cloud service such as CDN, WAF, or OBS. For details, see [Adding a CNAME Record Set](#).
3. Configure 301/302 redirection for the website IP address to redirect example.net to www.example.net.

Accessing a mailbox: Add an MX record set and an A record set for example.net. The MX record set configured for example.net does not conflict with the A record set. For details, see [Adding an MX Record Set](#).

(Not Recommended) Alternative Solution

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

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

You can refer to the following configuration:

Accessing a website: Add a CNAME record set for example.net to map the domain name to the domain name of the cloud service such as CDN, WAF, or OBS.

Accessing a mailbox: Add an MX record set for example.net using a different line to avoid conflicts with the CNAME record set.

 **WARNING**

This solution cannot prevent the situation where the mailbox may become unavailable. Evaluate the risks carefully.

4.3 How Do I Add Record Sets to Subdomains?

To resolve a subdomain, you need to enter a prefix for the second-level domain name when you configure a record set for it.

The following uses example.com to describe how to add an A record set to its subdomain 123.example.com to map it to an IPv4 address 192.168.1.2.

 **NOTE**

To translate 123.example.com to 192.168.1.2, you need to set the **Name** field to **123** when you add the A record set to example.com. The number of subdomains under a second-level domain name depends on the number of record sets that can be configured for the second-level domain name.

By default, each account can add a maximum of 500 record sets. You can view the number of record sets that can be added above the record set list.

If the quota fails to meet your requirements, contact customer service to request a higher quota.

Procedure

1. Go to the [Public Zones](#) page.
2. Click the domain name example.com.
3. Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.
4. Configure the parameters based on [Table 4-3](#).

Table 4-3 Parameters for adding an A record set

Parameter	Description	Example Value
Name	Prefix of the second-level domain name. (You do not need to enter the second-level domain name.)	123
Type	Type of the record set.	A – Map domains to IPv4 addresses

Parameter	Description	Example Value
Line	<p>Resolution line.</p> <p>The DNS server will return the IP address of the specified line based on the source of visitors.</p> <ul style="list-style-type: none"> • Default: returns the default resolution result irrespective of where the visitors come from. • ISP: returns the resolution result based on visitors' carrier networks. For details, see Configuring ISP Lines. • Region: returns the resolution result based on visitors' geographical locations. For details, see Configuring Region Lines. 	Default
TTL (s)	Cache duration of the record set, in seconds.	300
Value	IPv4 addresses mapped to the domain name. Enter each IPv4 address on a separate line.	10.18x.xxx.xxx
Weight	<p>(Optional) Weight of a record set.</p> <p>The value ranges from 0 to 1000, and the default is 1.</p> <p>This parameter is only designated for public domain names.</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.</p>	1
Tag	<p>(Optional) This parameter is displayed when you expand More Settings. Identifier of the record set. Each tag contains a key and a value. You can add a maximum of 10 tags to a record set.</p> <p>For details about tag key and value requirements, see Table 4-4.</p>	example_key1 example_value1
Description	(Optional) Supplementary information about the record set.	-

Table 4-4 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 a maximum of 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 a maximum of 43 characters. • Cannot start or end with a space nor contain special characters =*⟨>\\,/ 	example_value 1

5. Click **OK**.

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

4.4 Which IP Address Is Returned for the Domain Name If There Are Multiple IP Addresses in a Record Set?

You can configure multiple IP addresses in A and AAAA record sets.

If you have configured multiple IP addresses for an A or AAAA record set, all configured IP addresses will be returned for each query in a random sequence, and the first IP address will be used.

The following describes how a domain name is resolved:

1. An end user enters a domain name in a browser, and the request for the domain name is sent to the local DNS server.
2. The local DNS server forwards the request to the authoritative DNS server.
3. The authoritative DNS server returns all IP addresses to the local DNS server in a random sequence.
4. The local DNS server returns all IP addresses to the browser.
5. The browser uses the first IP address for connection.

Statistically, the probability of returning each IP address is approximately the same.

The following is an example how IP addresses are returned for a domain name. You have a website with a domain name of example.com and deployed on three servers. The IP addresses of the three servers are 192.168.1.1, 192.168.1.2, and 192.168.1.3.

An A record set is configured for example.com, with the **Value** field set to the three IP addresses.

Table 4-5 describes the IP addresses returned when different end users access the website.

Table 4-5 IP addresses returned for the domain name

End User	IP Addresses Returned by the Local DNS Server	IP Address Accessed by the Browser
User A	192.168.1.1 192.168.1.2 192.168.1.3	192.168.1.1
User B	192.168.1.2 192.168.1.1 192.168.1.3	192.168.1.2
User C	192.168.1.3 192.168.1.1 192.168.1.2	192.168.1.3

4.5 Can I Modify a Zone?

Yes. You can modify only the email address and its description of a created zone.

4.6 Can DNS Translate a Domain Name to IP Addresses of On-premises Servers or Third-Party Servers?

Yes. DNS can map a domain name and its subdomains to IP addresses of Huawei Cloud servers, third-party servers, or on-premises servers as long as the record sets are correctly configured.

For example, when you [add an A record set](#), ensure that the record set value is set to IPv4 addresses bound to the servers.

4.7 How Can Multiple Domain Names Be Linked to the Same Website?

To access a website using a domain name, host the domain name in the DNS service and configure an A record set to map the domain name to the IP address of the web server where the website is deployed.

To access the same website using other domain names, you need to configure an A record set with the same value for each domain name. [Table 4-6](#) provides an example.

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

Table 4-6 Example record sets

Domain Name	Record Set Type	Value
example1.com	A	192.168.1.1
example2.com		

4.8 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.

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.

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 4-7 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** page is displayed.
3. Click **Add Record Set**.

Figure 4-3 Setting weights

✕

Add Record Set

Name ?

* Type

* Line ?

* TTL (s) 5 min 1 h 12 h 1 day ?

* Value

Example:
192.168.10.10

?

Weight ?

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

10 tags available for addition.

Description 0/255

4. Configure the parameters as follows:
 - **Name:** Leave this parameter blank. The DNS service automatically considers example.com as the name, and requests are routed to 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.

4.9 Can DNS Resolve a Domain Name that Has Not Been Licensed?

After you register a domain name and complete the real-name authentication for the domain name, you can configure record sets for the domain name. Whether DNS can resolve the domain name depends on the location where the website that uses the domain name operates.

- The website operates within the Chinese mainland.

According to the *Measures for the Administration of Internet Information Services* issued by MIIT, all websites with their own domain name that operate inside Chinese mainland are required to obtain a license, and Internet service providers are required to block the site if a license is not acquired within a grace period.

Before you configure record sets for the domain name, obtain a license for your website. Otherwise, access to the website using the domain name will be blocked.

NOTE

If you have configured record sets for the domain name before the website is licensed, [suspend the domain name resolution by disabling the record sets](#). Otherwise, the license cannot be obtained.

- The website operates outside the Chinese mainland.

Websites outside the Chinese mainland do not need to be licensed. You can directly configure record sets for the domain name.

4.10 Does DNS Support Dynamic Domain Name Resolution?

No. DNS can only translate domain names to fixed IPv4 and IPv6 addresses.

4.11 How Do I View and Change the DNS Servers of a Domain Name?

Scenarios

The DNS server addresses of a domain name determine the DNS service provider for domain resolution on the Internet.

After you configure record sets for a public domain name and its subdomains, you need to check whether their DNS server addresses are those provided by Huawei Cloud DNS at the domain name registrar. If the DNS server addresses are not those provided by Huawei Cloud DNS, the domain names will not be resolved.

The following are operations for you to view and change the DNS server addresses of a domain name.

By default, Huawei Cloud DNS is used to resolve domain names registered with Huawei Cloud.

Changing the DNS Server Address of the Huawei Cloud Domain Name

For domain names registered with Huawei Cloud, you can log in to the DNS console to check whether they are correctly resolved.

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

If your domain name is hosted on Huawei Cloud DNS, set **DNS Server** to the Huawei Cloud DNS server address.

- 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 Server Addresses for Domain Names Registered with Other Service Providers

If a domain name is registered and managed by another registrar, go to the domain name management page of the registrar and change the DNS server addresses to specified ones.

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.

5 Private Zones

5.1 Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?

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

[Table 5-1](#) lists the rules.

Table 5-1 Restrictions between record types

	CNAME	A	AAAA	MX	TXT	PTR	SRV
CNAME	Repeat	Conflict	Conflict	Conflict	Conflict	Conflict	Conflict
A	Conflict	Repeat	No limit	No limit	No limit	No limit	No limit
AAAA	Conflict	No limit	Repeat	No limit	No limit	No limit	No limit
MX	Conflict	No limit	No limit	Repeat	No limit	No limit	No limit
TXT	Conflict	No limit	No limit	No limit	Repeat	No limit	No limit
PTR	Conflict	No limit	No limit	No limit	No limit	Repeat	No limit
SRV	Conflict	No limit	No limit	No limit	No limit	No limit	Repeat

The rules are as follows:

- **Repeat:** A record set of the same type already exists, and record sets of the same type can be added.
- **Conflict:** The two types of record sets cannot have the same resolution line.
- **No limit:** The two types of record sets can coexist.

If the message is displayed, perform the following operations:

- Delete the existing record set that conflicts with the record set that you want to add, and then add the record set back.

NOTE

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

- Set a different name for the record set.

5.2 How Do I Change Default DNS Servers of an ECS to Huawei Cloud Private DNS Servers?

Huawei Cloud provides private DNS servers for domain name resolution in VPCs. ECSs use public domain names to access the Internet, but use private domain names to access cloud services like OBS and SMN, with no need to connect to the Internet.


For ECSs created before private DNS was available, public DNS server addresses (for example, 114.114.114.114) are configured for VPC subnets of the ECSs by default. To allow ECSs on these subnets to use private domain names, change the default public DNS server addresses to those of Huawei Cloud private DNS servers. For details about private DNS servers, see [What Are Huawei Cloud Private DNS Server Addresses?](#)

Viewing the DNS Server Addresses for an ECS

1. Log in to the management console.
2. Choose **Computing > Elastic Cloud Server**.
The **Elastic Cloud Server** page is displayed.
3. In the ECS list, click the name of the target ECS.
4. On the ECS details page, click the VPC name.
The **Virtual Private Cloud** page is displayed.
5. Locate the VPC and click the number in the **Subnets** column.
The **Subnets** page is displayed.
6. Click the name of the subnet.
In the **Gateway and DNS Information** area, view the DNS server addresses used by the ECS.

Changing the DNS Server Addresses for a VPC Subnet

If the ECS uses default public DNS server addresses, change them to Huawei Cloud private DNS server addresses.

1. In the **Gateway and DNS Information** area, click  next to **DNS Server Address**.
2. Change the DNS server addresses to private DNS server addresses.

Updating the DNS Server Addresses for the ECS

New DNS server addresses will take effect after they are updated. There are two ways to do this:

- Restart the OS. The ECS will then obtain the new DNS server addresses from the DHCP server.

NOTICE

Restarting the OS will interrupt services on the ECS. Perform this operation during off-peak hours.

Alternatively, wait for the DHCP lease to expire, which is 365 days by default. After the lease time expires, the DHCP server allocates another IP address and updates the DNS server addresses to the ECS.

- Manually change the DNS settings on the ECS.

If DHCP is disabled on the ECS, manually update DNS settings.

For example, if the ECS is running Linux, change the DNS settings by editing the `/etc/resolv.conf` file.

5.3 How Can I Access an ECS Using Its Host Name?

The DNS service allows you to create private zones for any top-level domain names except `.com`.

If you set the name of an ECS to `ecs01`, you can create a private zone for `ecs01` and add an A record to map `ecs01` to the private IP address of the ECS so that the ECS can be accessed using its host name.

Procedure

1. Go to the [Private Zones](#) page.
2. Click **Create Private Zone**. In the displayed dialog box, set the domain name to `ecs01`.
3. Click **OK**.
You can view the created private zone on the **Private Zones** page.
4. Click the domain name.
The **Record Sets** page is displayed.
5. Click **Add Record Set**.
Add an A record set to the zone.
 - Set **Type** to **A - Map domains to IPv4 addresses**.
 - Leave the **Name** field blank.

- Set **Value** to the private IP address of the ECS, for example, **192.168.1.10**.
6. Click **OK**.
After the record set is added, you can use ecs01 to access the ECS whose private IP address is 192.168.1.10 in the associated VPC.

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

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

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

To add a PTR record, you may refer to [Creating a PTR Record](#).

NOTE

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

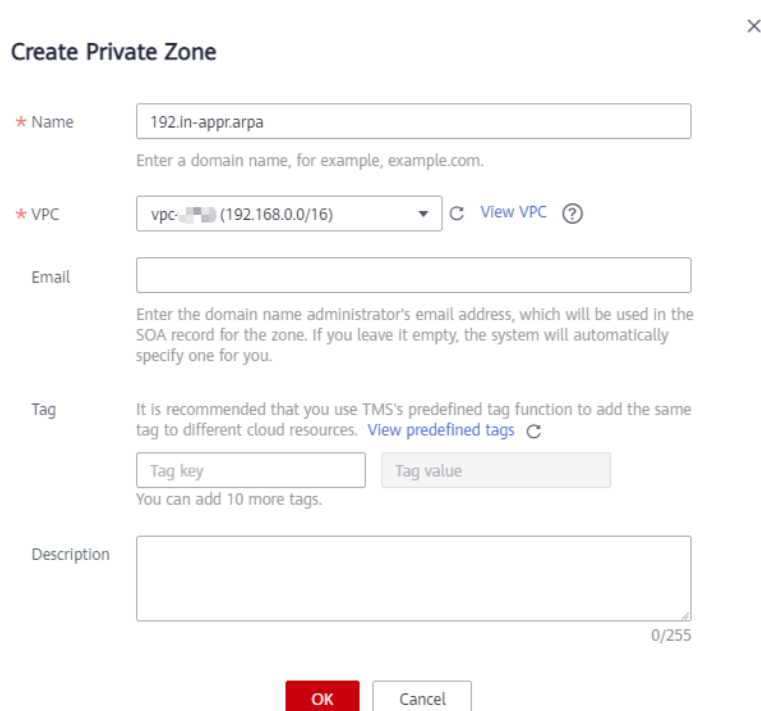
For example, if the private IP address is 192.168.1.10, the domain name is 10.1.168.192.in-addr.arpa.

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

Creating a Private Zone

1. Go to the [Private Zones](#) page.
2. Click **Create Private Zone**.

Figure 5-1 Create Private Zone



Create Private Zone ×

★ Name
Enter a domain name, for example, example.com.

★ VPC
View VPC ?

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.

Tag It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#)

You can add 10 more tags.

Description
0/255

- Configure the parameters based on [Table 5-2](#).

Table 5-2 Parameters for creating a private zone

Parameter	Description	Example Value
Domain Name	Domain name you use to access the cloud servers or cloud services. Ensure that the domain name suffix is in-addr.arpa .	192.in-addr.arpa
VPC	VPC to be associated with the private zone. Select the VPC you want to associate with the private zone.	-
Email	(Optional) Email address of the administrator managing the private zone. Recommended email address: HOSTMASTER@Domain name For more information about the email address, see Why Was the Email Address Format Changed in the SOA Record?	HOSTMASTER@example.com

Parameter	Description	Example Value
Tag	<p>(Optional) Identifier of a resource.</p> <p>Each tag contains a key and one or more values. You can add a maximum of 10 tags to a zone.</p> <p>For details about tag key and value requirements, see Table 5-3.</p> <p>NOTE If you have configured tag policies for DNS, 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</p> <p>example_value1</p>
Description	<p>(Optional) Supplementary information about the zone.</p> <p>You can enter a maximum of 255 characters.</p>	<p>This is a private zone.</p>

Table 5-3 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 a maximum of 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 a maximum of 43 characters. Cannot start or end with a space nor contain special characters =* <> \, / 	<p>example_value1</p>

4. Click **OK**.
5. Switch back to the **Private Zones** page.
You can view the created private zone in the private zone list.

 **NOTE**

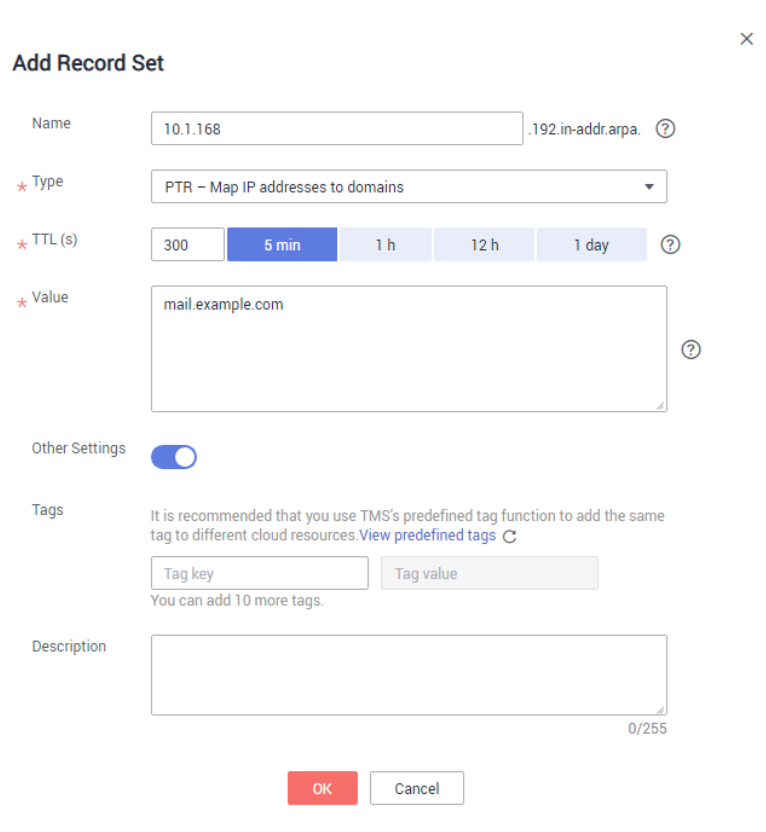
You can click the domain name to view SOA and NS record sets automatically generated for the zone.

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

Adding a PTR Record

1. On the **Private Zones** page, click the domain name of the private zone you created.
The **Record Sets** page is displayed.
2. Click **Add Record Set**.
The **Add Record Set** dialog box is displayed.

Figure 5-2 Add Record Set



Add Record Set [X]

Name: 10.1.168 .192.in-addr.arpa. [?]

* Type: PTR - Map IP addresses to domains [v]

* TTL (s): 300 5 min 1 h 12 h 1 day [?]

* Value: mail.example.com [?]

Other Settings:

Tags: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) [C]

Tag key: [] Tag value: []

You can add 10 more tags.

Description: [] 0/255

[OK] [Cancel]

3. Configure the parameters based on [Table 5-4](#).

Table 5-4 Parameters for adding a PTR record

Parameter	Description	Example Value
Name	Part of the private IP address in reverse order.	10.1.168 For example, if the IP address is 192.168.1.10, the domain name in the PTR record must be 10.1.168.192.in-addr.arpa. <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.
Type	Type of the record set.	PTR – Map IP addresses to domains
TTL (s)	Cache duration of the record set, in seconds.	Default value: 300
Value	Domain name mapped to the IP address. You can enter only one name.	mail.example.com
Tag	(Optional) Identifier of a record set. Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. For details about tag key and value requirements, see Table 5-3 . NOTE If you have configured tag policies for DNS, 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 PTR record set. This parameter is displayed when you expand More Settings .	The PTR record is for reverse resolution.

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

5.5 How Can I Use a Private Domain Name to Route Internet Traffic?

You can use a domain name to route traffic over the Internet or within VPCs.

Private DNS translates domain names in VPCs and forward DNS queries for public domain names to public DNS servers. The following describes how an ECS accesses a website using a domain name.

- If the domain name is a private domain name you configure on the DNS console or is the domain name of a cloud service, private DNS directly returns the mapped IP address.
- If the domain name has been registered with a domain name registrar, private DNS forwards the request to a public DNS server (for example, 114.114.114.114) and then returns the mapped IP address to the ECS.

If the public domain name is the same as the private domain name, requests to the public domain name will be handled by a private DNS server. If no IP address is found, private DNS will return a message indicating that no record was found and will not forward the request to the public DNS server.

To address this issue, you can use a subdomain of the public domain name as the private domain name and add record sets for the subdomain.

If the public domain name is example.com, create a private zone for subdomain 123.example.com and configure record sets for 123.example.com. In this way, requests to 123.example.com and all its subdomains (*.123.example.com) are processed by the private DNS server, and requests to example.com and other subdomains are forwarded to the public DNS server.

NOTE

- If Huawei Cloud DNS is used for domain name resolution over public networks, you can create a public zone example.com and add record sets for it. For details, see [Routing Internet Traffic to a Website](#).
- If you select another DNS service provider, see the help documentation of that provider.
- For details about how to configure a private zone for subdomain 123.example.com on the DNS console, see [Routing Traffic Within VPCs](#).

5.6 Can I Use Private Domain Names Across Regions?

Private zones are region-level resources. They are created in specified regions and projects.

A private zone can be associated with more than one VPC and takes effect only in its associated VPCs. However, a private zone cannot be used across VPCs. If these VPCs are in the same region and connected over a [VPC peering connection](#), the private zone can be accessed across VPCs.

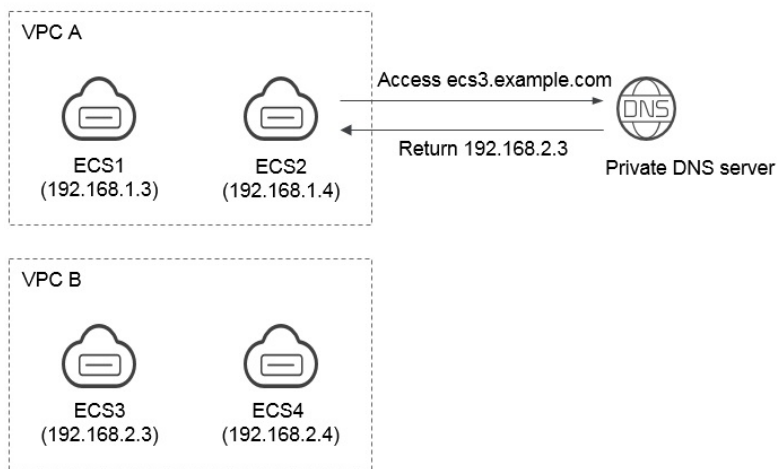
In the following example, a private zone is created for domain name **example.com**, and it has two VPCs associated and two record sets.

Table 5-5 Record sets added to private zone example.com

Domain Name	Type	Value
ecs1.example.com	A	192.168.1.3
ecs3.example.com	A	192.168.2.3

Figure 5-3 shows how the private domain name is resolved.

Figure 5-3 Process for resolving a private domain name



All ECSs in VPC A and VPC B can access example.com.

If ECS 2 in VPC A accesses ecs3.example.com, the private DNS server returns 192.168.2.3, the IP address of ECS 3 in VPC B. There is no VPC peering connection between VPC A and VPC B. ECS 2 cannot access ECS 3 in VPC B using this IP address.

5.7 Do I Need to Register Private Domain Names?

Private domain names only take effect in associated VPCs. You do not need to register them.

You can customize any private domain name, other than .com, as long as it complies with domain name specifications. All private domain names are free.

5.8 Will a Deleted VPC Be Automatically Disassociated from the Private Zone?

No. Deleted VPCs will not be automatically disassociated from the private zones. If you delete a VPC that has been associated with a private zone, you need to manually disassociate it from the private zone.

5.9 Are Private DNS Server Addresses the Same for All Users?

Private DNS server addresses are the same in the same AZ, and private domain names of each user are logically isolated.

5.10 What Are the Restrictions on Concurrent Private DNS Requests?

To ensure the lookup efficiency of private domain names, only 2,000 queries are allowed on a single source IP address per second. If a server initiates DNS queries with an overwhelmingly high frequency, significantly in excess of normal service demands, and there are more than 2,000 queries per second, additional queries will not be processed.

If your services initiate an enormous volume of concurrent requests, enable DNS caching to improve lookup efficiency.

 **CAUTION**

If you have special services where access to a large number of Internet domain names is required, some domain names may not be accessed due to traffic limiting. To avoid this, [submit a service ticket](#).

6 Reverse Resolution

6.1 What Is Reverse Resolution?

Generally, DNS resolves a domain name to an IP address. When you access a website using a domain name, DNS maps the domain name to the IP address of the web server where the website is deployed.

Reverse resolution, on the opposite, is a query in which a domain name connected with an IP address is returned. It is usually used in scenarios such as anti-spam and logging.

- Anti-spam: queries the domain name based on the IP address of the sender's mail server to obtain the reputation of the domain name.
- Logging: queries the domain name or host name based on the IP address to distinguish service data.

To obtain a domain name from a private IP address, you need to create a private zone for top-level domain in-addr.arpa. For example, if the IP address 192.0.2.255, the domain name for the PTR record can be 255.2.0.192.in-addr.arpa.

By default, each EIP supports reverse resolution, and its domain name for the PTR record is in the format of **ecs-x-x-x-x.compute.hwclouds-dns.com**. By pinging each EIP, you can obtain its default domain name. You can create a PTR record for the EIP to overwrite the default domain name.

7 Domain Transfer

7.1 Can I Transfer a Hosted Public Domain Name from One Account to Another Account?

No. You are not allowed to transfer a public domain name hosted on the DNS service from one account to another account.

If you have [created a public zone](#) and [added record sets to the public zone](#), you cannot transfer the domain name from one account to another account.

NOTE

If you want to transfer a hosted domain name to another account, [delete the public zone](#) created under the current account, create the same public zone under the new account, and add record sets to the public zone. This operation will interrupt domain name resolution. Exercise caution when performing this operation.

7.2 How Do I Migrate My Domain from Another DNS Service Provider to Huawei Cloud DNS?

You can migrate a domain name to Huawei Cloud DNS from another DNS service provider.

Procedure

1. Create a public zone.

Before you migrate your domain name, create a public zone for the domain name on the DNS console.

For details, see [Routing Internet Traffic to a Website](#).

NOTE

After you create a public zone, the system automatically creates the NS and SOA record sets, which are used to query information about the authoritative DNS servers.

2. Add record sets.

 NOTE

Migrate record sets of the domain name to the DNS service. You can export them from your current DNS service provider and import them to the DNS service.

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

3. Run the following command to check whether a DNS record has taken effect:
 - For Windows OS
nslookup [-qt=*Record set type*] [*Domain name*] [*Authoritative DNS server*]
 - For Linux OS
dig [*Record set type*] [*Domain name*] @[*Authoritative DNS server*]
4. 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.
5. Wait for the change to take effect.

Generally, changes to DNS server addresses are quickly updated to top-level DNS servers and take effect on the Internet. However, some domain name registrars set the TTL value for NS records to 48 hours. If the NS records are cached by a local DNS server, the changes would take effect in 48 hours.

You can check the accurate time on the DNS service provider's website. Do not delete original record sets until the changes take effect. In this case, even if the change does not take effect, your services will not be interrupted.

8 Change History

Released On	Description
2022-06-21	<p>This issue is the ninth official release, which incorporates the following changes:</p> <ul style="list-style-type: none"> • Added How Do I View and Change the DNS Servers of a Domain Name? • Modified What Is Reverse Resolution?
2020-06-17	<p>This issue is the eighth official release, which incorporates the following changes:</p> <ul style="list-style-type: none"> • Classified FAQ. • Added the following section: <ul style="list-style-type: none"> – What Are the Priorities of Resolution Lines? – Does DNS Support Dynamic Domain Name Resolution? – When Will New DNS Server Addresses Take Effect? • Modified the following content: <ul style="list-style-type: none"> – Added conflict examples and solutions in Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set? – Optimized Can I Transfer a Hosted Public Domain Name from One Account to Another Account?
2020-02-21	<p>This issue is the seventh official release, which incorporates the following changes:</p> <p>Added new DNS addresses in What Are Huawei Cloud DNS Servers?</p>
2020-02-12	<p>This issue is the sixth official release, which incorporates the following changes:</p> <ul style="list-style-type: none"> • Added examples in How Do I Check Whether a Record Set Has Taken Effect? • Added restrictions on NS and CNAME record set conflicts in Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?

Released On	Description
2019-09-05	<p>This issue is the fifth official release, which incorporates the following changes:</p> <p>Added the private DNS server addresses in the LA-Santiago region in What Are Huawei Cloud Private DNS Server Addresses?</p> <p>Added the following content:</p> <ul style="list-style-type: none"> ● Can I Transfer a Hosted Public Domain Name from One Account to Another Account? ● Can DNS Translate a Domain Name to IP Addresses of On-premises Servers or Third-Party Servers? ● Does DNS Support Explicit and Implicit URLs? ● Why Can't I Access the Website Even Though the Domain Name Has Been Resolved? ● What Are the Differences Between Public and Private Domain Names? ● How Can I Use a Private Domain Name to Route Internet Traffic? ● Can I Use Private Domain Names Across Regions? ● How Do I Add Record Sets to Subdomains? ● Does DNS Support IPv6?
2019-08-23	<p>This issue is the fourth official release, which incorporates the following changes:</p> <p>Updated the private DNS server addresses in the AP-Singapore region in What Are Huawei Cloud Private DNS Server Addresses?</p>
2019-07-02	<p>This issue is the third official release, which incorporates the following changes:</p> <p>Optimized the following FAQs:</p> <ul style="list-style-type: none"> ● How Do I Change Default DNS Servers of an ECS to Huawei Cloud Private DNS Servers? ● What Is TTL? ● What Are the Restrictions on Concurrent Private DNS Requests?
2019-03-05	<p>This issue is the second official release, which incorporates the following changes:</p> <ul style="list-style-type: none"> ● Updated the screenshots. ● Added DNS server addresses in different regions in What Are Huawei Cloud Private DNS Server Addresses?
2018-11-22	<p>This issue is the first official release.</p>