Domain Name Service

FAQs

Issue 01

Date 2022-06-17

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Will I Be Billed for the DNS Service?

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

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

By default, you can use an account to create up to 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 to request an increased quota.

1.3 What Are DNS Server Addresses Provided by Huawei Cloud DNS?

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

Huawei Cloud DNS Servers

To enable users to access the nearest DNS server and resolve domain names with the lowest latency, Huawei Cloud has deployed DNS servers in multiple AZs around the world and support anycast in some regions.

The following are addresses used by DNS servers:

- ns1.huaweicloud-dns.com: DNS server address for regions in the Chinese mainland
- ns1.huaweicloud-dns.cn: DNS server address for regions in the Chinese mainland

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

After you **create a public zone** on the console, an NS record set is automatically generated for the zone, and its value is the four DNS server addresses.

Suggestions on DNS Address Setting

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

Follow the following suggestions to set the NS record set for the public zone:

- If your website users are mainly in the Chinese mainland, set the DNS server addresses to ns1.huaweicloud-dns.com and ns1.huaweicloud-dns.cn.
- If your website users are mainly in countries or regions outside the Chinese mainland, set the DNS addresses to ns1.huaweicloud-dns.net and ns1.huaweicloud-dns.org.
- If your website users are all over the world, configure all four DNS server addresses.

Setting DNS Server Addresses

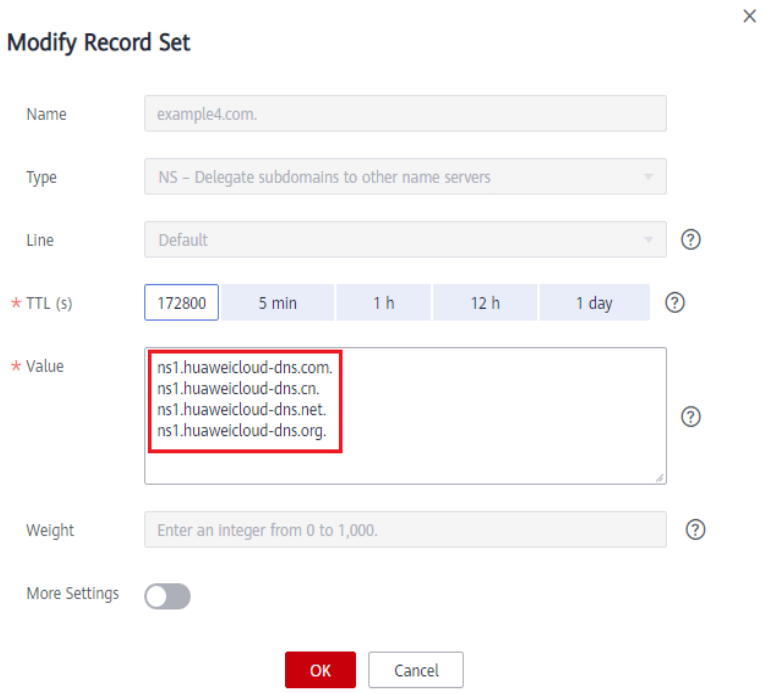
Set the DNS server addresses on the **Record Sets** page.

1. Log in to the management console.
2. Hover the cursor over  in the upper left corner. In the service list, choose **Networking** > **Domain Name Service**.

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

   The **Public Zones** page is displayed.
4. In the public zone list, click the name of the zone whose record sets you want to modify.
5. On the **Record Sets** page, locate the NS record set that was automatically generated by the system and click **Modify** under **Operation**.

Figure 1-1 Modify Record Set



6. Change the settings of **Value** based on **Suggestions on DNS Address Setting**.
7. Click **OK**.

NOTE

ns1.hwclouds-dns.com and ns1.hwclouds-dns.net were originally registered with Huawei Cloud and can still be used, but they may not perform as well as the four new servers listed near the beginning of this FAQ.

1.4 What Are the Private DNS Server Addresses Provided by Huawei Cloud?

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 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, as shown in **Table 1-1**.
- 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
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
AF-Johannesburg	100.125.1.250
	100.125.1.14

Region	Private DNS Server Address
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

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?

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

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 itself is also available over either IPv4 or IPv6. Huawei Cloud provides the following DNS servers: ns1.huaweicloud-dns.com, ns1.huaweicloud-dns.cn, ns1.huaweicloud-dns.net, and ns1.huaweicloud-dns.org

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

1.7 Does DNS Support Explicit and Implicit URLs?

Huawei Cloud DNS does not support URL forwarding.

Explicit and implicit URL forwarding is not performed over a standard DNS protocol, but 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?

DNS can translate domain names to fixed IPv4 and IPv6 addresses.

1.9 Does DNS Support Wildcard Entries?

DNS allows you to configure wildcard entries.

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

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

1.10 What Is TTL?

TTL is short for time to live. It 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. The local DNS servers for ECSs purchased on Huawei Cloud are private DNS servers. For details, see **What Are the Private DNS Server Addresses Provided by Huawei Cloud?**

When the local DNS server receives a domain name request, it asks the authoritative DNS server of the domain name for the required resource 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 does not request the record from the authoritative DNS server, but directly returns a result from the record in its cache.

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

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

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:

- Custom lines enjoy the highest priority, and ISP lines take precedence over region lines. The priorities of the four 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 period (.) and includes a backslash (\) before the period in the label before the at sign, but emails are still sent to the email address you specify. For more information, see RFC 1035.

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

1.15 What Is CAA?

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

CAA Specifications

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

For security reasons, only authorized CAs can issue SSL certificates for the domain names used by your website. Setting CAA records enhances security for your website.

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

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

  Any other CAs can also issue certificates for this domain name. Insecure certificates may be issued, and messages indicating that your website is insecure when users access your website.
- If the CA finds a CAA record that authorizes it to issue certificates, it will issue a certificate for the domain name.
- If the CA finds a CAA record but the record does not authorize it to issue certificates, the CA will not be able to issue SSL certificates for the domain name.

CAA Record

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

Table 1-3 Configuration of CAA records

Function	Example	Description
Configure a CAA record 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**.
Configure the CA to report violations to the domain name holder.	0 iodef "mailto:admin@domain.com"	If a certificate request violates the CAA record, 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 specified CA (**ca.example.com**) can issue wildcard certificates for the domain name.

Function	Example	Description
Configuration example	0 issue "ca.abc.com" 0 issuewild "ca.def.com" 0 iodef "mailto:admin@domain.com"	The example configures a CAA record for the domain name **domain.com**. • 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. • When a violation occurs, the CA sends a notification to **admin@domain.com**.

Checking Whether a CAA Record Has Taken Effect

Use Domain Information Groper (dig) to check whether the CAA record 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 What Is the MX Record Set Priority?

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?

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 Should I Do If a Record Set Does Not Take Effect?

Symptom

If no IP address is returned when you ping a domain name, the record set has not taken effect. There are multiple causes for the resolution failure. This section describes how to troubleshoot the resolution failure.

Fault Locating

The issues here are described in order of how likely they are to occur.

Troubleshoot the issue by ruling out the causes described here, one by one.

1. **Checking Whether the Zone Status Is Normal**: Check whether the zone has expired and whether its status is normal.
2. **Checking Whether the DNS Address of the Domain Name Is the Huawei Cloud DNS Address**: If the domain name is set to be resolved by a non-Huawei Cloud DNS address, the domain name cannot be resolved.
3. **Checking Whether a Record Set Is Correctly Added**: Check whether the record sets configured for the domain name are correct.
4. **Checking Whether the DNS Server of the Domain Name Has Been Changed Within 24 Hours**: The carrier's local DNS server caches the NS record of the domain name. It takes a maximum of 48 hours to update the NS record.
5. **Checking Whether the Authoritative DNS Resolution Takes Effect**: Run the **nslookup** command to check whether the record sets of the domain name take effect on the authoritative DNS server.
6. **Submitting a Service Ticket**

Checking Whether the Zone Status Is Normal

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 Whether the DNS Address of the Domain Name Is the Huawei Cloud DNS Address

The DNS service provides authoritative DNS servers for domain resolution.

If a non-Huawei Cloud DNS address is configured for the domain name, the domain name cannot be resolved.

Checking Whether a Record Set Is Correctly Added

1. Log in to the **DNS console** and check the zone status.

   If the resolution is suspended, the domain name cannot be resolved.

2. Check whether record sets have been added and whether their status is **Normal**.

   For example, if www.xxx.com cannot be accessed, the possible cause is that only the record set for xxx.com is added and the record set for www is not added.

Checking Whether the DNS Server of the Domain Name Has Been Changed Within 24 Hours

The modification of the DNS server does not take effect immediately. The TTL value of NS records is usually set to 48 hours by domain name registrars. In this scenario, if the local DNS server caches the NS record of a 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 Whether the Authoritative DNS Resolution Takes Effect

Run the following command to check whether record sets of the domain name take effect on the authoritative DNS server:

nslookup -qt= *Type Domain name Authoritative DNS address*

Take **ns1.huaweicloud-dns.cn** as an example. To check whether record sets of domain name **example.com** take effect on the authoritative DNS server, 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 cannot be returned when the domain name is used for access, the local DNS server may be hijacked. Run either of the following commands to check whether the public DNS resolution takes effect: **nslookup -qt=***Type Domain name* **8.8.8.8** or **nslookup -qt=***Type Domain name* **114.114.114.114**

If the public DNS resolution takes effect, you are advised to 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 Record Sets Have Taken Effect?

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

After a record set is added for a domain name, the record set takes effect only after it is synchronized to the DNS server.

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

  If a carrier forcibly prolongs the cache time of domain name record sets, the effective time will be slightly delayed.

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

Run the following commands to check whether a record set has taken effect:

- **ping** *Domain name*
- **nslookup -qt=***Type Domain name*

For details, see

- **Running the Ping Command to Check Whether a Record Set Has Taken Effect (Applicable to Windows or Linux Hosts)**
- **Running the nslookup Command to Check Whether a Record Set Has Taken Effect (Applicable to Windows and Linux Hosts)**

Running the Ping Command to Check Whether a Record Set Has Taken Effect (Applicable to Windows or Linux Hosts)

1. On your local host, click the search icon and enter **cmd** to open the CLI.
2. Run the following commands to check whether the record sets take effect:

   ping *Domain name*

   For example, to check whether the resolution of domain name example.com has taken effect, run the **ping example.com** command.

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

Running the nslookup Command to Check Whether a Record Set Has Taken Effect (Applicable to Windows and Linux Hosts)

- **Verify an A record set.**

a. On your local host, click the search icon and enter **cmd** to open the CLI.
b. Run the following commands to check whether the record sets take 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 takes effect.

- **Verify a CNAME record set**: Content Delivery Network (CDN), Web Application Firewall (WAF), and CloudSite scenarios.
  a. On your local host, click the search icon and enter **cmd** to open the CLI.
  b. Run the following commands to check whether the record sets take effect:

     nslookup -qt=cname *domain name*

     Example: **nslookup -qt=cname examplesite.com**

     If the displayed CNAME value is the same as that configured in the record set, the record set takes effect.
- **Verify a MX record set**: It is used to specify the address of a mail server.
  a. On your local host, click the search icon and enter **cmd** to open the CLI.
  b. Run the following commands to check whether the record sets take 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 takes effect.
- **Verify a NS record set**: It is used to specify the DNS address of the resolution service provider.
  a. On your local host, click the search icon and enter **cmd** to open the CLI.
  b. Run the following commands to check whether the record sets take effect:

     nslookup -qt=ns *Domain name*

     Example: **nslookup -qt=ns example123.top**

     If the displayed IP address is the same as the DNS address of the service provider, the record set has taken effect.
- **Check whether the domain name resolution of a specified authoritative DNS server takes effect.**
  a. On your local host, click the search icon and enter **cmd** to open the CLI.
  b. Run the following commands to check whether the record sets take effect:

     nslookup -qt= *Type Domain name Authoritative DNS address*

     Example: Run the following command to check whether domain name example.com can be resolved by the authoritative DNS server (ns1.huaweicloud-dns.cn is used as an example):

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

The record sets of example123.com using authoritative DNS ns1.huaweicloud-dns.cn has taken effect.

FAQ

- If the correct IP address cannot be obtained during the verification, the record set has not taken effect or has been modified. You are advised to 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 opened.

  The possible cause is that the DNS resolution cache is not refreshed. Run the **ipconfig /flushdns** command to refresh the cache. Alternatively, wait until the DNS is refreshed and try again.
- The ping command has proved that the domain name resolution is normal, but the website cannot be opened.

  Check whether the domain name is correctly bound to the ECS where the website is deployed or whether the website has been licensed. Refer to

  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?

- If a record set is being added for the first time, it takes effect immediately.
- If you delete a record set and add it again, it will take effect after the cache for the deleted record set expires. The amount of time is controlled by the TTL value configured for the deleted record set.

  In some cases, the carrier may prolong the cache duration of a domain name.

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 of the original record set expires.

If the carrier sets a longer cache duration, the record set will take effect after this period of time elapses.

2.5 When Will New DNS Server Addresses Take Effect?

Changes to DNS server addresses can be quickly synchronized to the top-level domain name servers and then be 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.

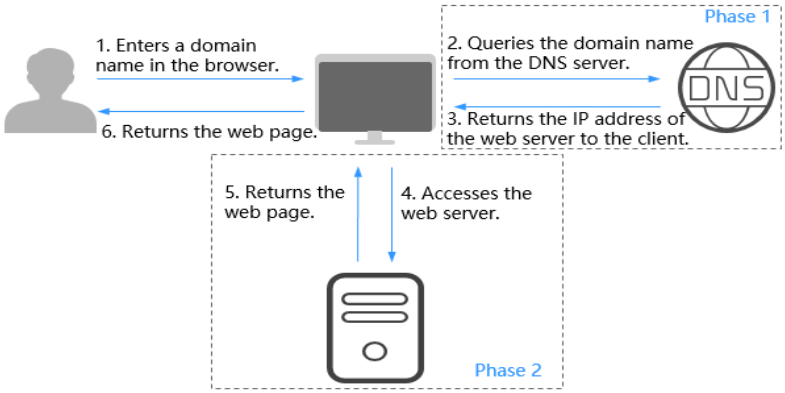
Consult the domain name registrars to learn how long the TTL has been configured for. Do not delete original record sets until the changes take effect to ensure your service continuity.

3 Website Access Failures

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

Figure 3-1 shows the process of accessing a website using a domain name.

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.

To successfully access a website, both phases are mandatory. If the web server is unavailable, the website cannot be accessed even if the DNS server has resolved the domain name.

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
a: NS record sets cannot be configured for primary domains like example.com. There is no such restriction on subdomains (for example, www.example.com). b: For primary domains like example.com, CNAME and NS record sets can coexist. For subdomains like www.example.com, CNAME record sets conflict with NS record sets.									

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.

NOTE

In the standard DNS FRC protocol, CNAME has the highest priority. If CNAME and other types (such as MX) coexist, CNAME records may hijack MX resolution records.

For example, CNAME resolution has been added to the local DNS and cached. When the client adds MX resolution (using the mailbox to send emails), the local DNS preferentially returns the CNAME cache instead of requesting MX resolution from the Internet. As a result, the mailbox fails to send emails.

You are advised to configure email domain names and website domain names at the same time. For example, if the level-1 domain name *xxx.com* is used as an email address, you do not need to add CNAME resolution for *xxx.com*. Instead, you can directly add an A record to resolve the domain name to the IP address.

4.2 How Do I Add Record Sets to Subdomains?

The procedure for adding record sets to a subdomain is the same as that for a primary domain name. You only need to enter a prefix for the domain name when you add record sets.

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 add a record set to a subdomain, you must enter a prefix for its primary domain name in the **Name** field. The number of subdomains that can be created under a primary domain name is the number of record sets that can be added to the hosted zone of the primary 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 quotas do not meet your service requirements, contact customer service to request an increased quota.

Procedure

1. Log in to the management console.
2. Hover the cursor over  in the upper left corner. In the service list, choose **Networking** > **Domain Name Service**.

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

   The zone list is displayed.
4. Click the name of the zone **example.com**.
5. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
6. Set required parameters based on **Table 4-2**.

Table 4-2 Parameters for adding an A record set

Parameter	Description	Example Value
Name	Prefix of the primary domain name. (You do not need to manually add the suffix.)	123
Type	Type of the record set.	A – Map domains to IPv4 addresses
Line	Resolution line. The DNS server will return the IP address of the specified line based on the source of visitors. • **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.	The default value is 300s, which is, 5 minutes.
Value	IPv4 addresses mapped to the domain name. Enter each IPv4 address on a separate line.	10.18x.xxx.xxx

Parameter	Description	Example Value
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default is **1**. This parameter is supported only for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set.	1
Tag	(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. For details about tag key and value requirements, see **Table 4-3**.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set. This parameter is displayed when you expand **More Settings**.	N/A

Table 4-3 Tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 characters. • Cannot start or end with a space or contain special characters =*<>\,|/	example_key1
Value	• Cannot be left blank. • Can contain a maximum of 43 characters. • Cannot start or end with a space or contain special characters =*<>\,|/	example_value1

7. Click **OK**.

   View the record set you added in the list and ensure that the status of the record set is **Normal**.

4.3 How Is a Domain Name Resolved When a Record Set Has Multiple Values?

Only A and AAAA record sets can have multiple values.

If an A or AAAA record set has multiple values, all IP addresses are returned for each query in a random sequence, and the first IP address is used.

The process how a domain name is resolved is as follows:

1. A visitor enters a domain name in a browser, and the request for the DNS query 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 randomly accesses one of the IP addresses. Generally, the first IP address is used.

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 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.

An A record set is added to the domain name, with the **Value** field set to the three IP addresses.

Table 4-4 describes the resolution results returned when different visitors access the website.

Table 4-4 Example resolution results

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

4.4 Can I Modify a Zone?

No. You can modify only the email address and its description.

4.5 Can DNS Translate a Domain Name to IP Addresses of On-premises Servers or Servers on Another Cloud?

You can add record sets to map a domain name and its subdomains to any server addresses within Huawei Cloud, on another cloud, or in on-premises equipment room. The domain name and its subdomains can be successfully resolved as long as the record set values are correct.

For example, when you **add an A record set**, ensure that the record set value is set to correct IPv4 addresses.

4.6 How Do I Access the Same Website Using Multiple Domain Names?

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 4-5** provides an example.

For details about how to add an A record set, see **Routing Internet Traffic to a Website**.

Table 4-5 Example record sets

Domain	Record Set Type	Value
example1.com	A	192.168.1.1
example2.com		
example3.com		

4.7 How Do I View and Change the DNS Address of a Domain Name?

Scenarios

The DNS service provides authoritative DNS servers for domain resolution.

After you add record sets for a domain name and sub-domain name, you need to check with your domain name registrar whether the DNS server addresses of the

domain name are those of Huawei Cloud DNS servers. If the DNS server address is incorrect, public domain name resolution cannot take effect. This section guides you to view and change the DNS address 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 address of the domain name.

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

   - ns1.huaweicloud-dns.com: DNS server address for regions in the Chinese mainland
   - ns1.huaweicloud-dns.cn: DNS server address for regions in the Chinese mainland
   - ns1.huaweicloud-dns.net: DNS server address for countries or regions outside the Chinese mainland
   - ns1.huaweicloud-dns.org: DNS server address 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 Private DNS Servers Provided by the DNS Service?

ECSs use private DNS servers for domain name resolution in VPCs. ECSs in a VPC can access the Internet using public domain names and other cloud services like OBS and SMN through private DNS servers, with no need to connect to the Internet.

Public DNS servers (for example, 114.114.114.114) are configured VPC subnets created earlier by default. To allow ECSs on these subnets to access private domain names, change the default public DNS servers to private DNS servers provided by the DNS service. For details about private DNS servers, see **What Are the Private DNS Server Addresses Provided by Huawei Cloud?**

Perform the operations provided in this FAQ to change the public DNS servers to private DNS servers.

Checking the DNS Server Addresses of an ECS

1. Log in to the management console.
2. In the **Computing** category, click **Elastic Cloud Server**.

   The **Elastic Cloud Server** page is displayed.
3. In the ECS list, click the ECS name.
4. On the ECS details page, click the VPC name.

   The **Virtual Private Cloud** page is displayed.
5. Locate the target VPC and click the number in the **Subnets** column.

   The **Subnets** page is displayed.
6. Click the name of the target subnet.

   In the **Gateway and DNS Information** area, view the DNS server addresses used by the ECS.

Changing the DNS Servers for a VPC Subnet

If the ECS uses default public DNS servers, change them to private DNS servers provided by the DNS service.

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 not take effect immediately on the ECS.

The DNS server addresses need to be updated first. 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 configurations on the ECS.

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

  For example, if the ECS is running Linux, change the DNS configurations 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 in VPCs except .com.

When you buy an ECS, you set a host name for it, for example, **ecs01**. You can then create a private zone named **ecs01** and add an A record to map the host name (**ecs01**) of the ECS to its private IP address so that the ECS can be accessed using its host name.

Procedure

1. Log in to the management console.
2. Hover the cursor over  in the upper left corner. In the service list, choose **Networking** > **Domain Name Service**.

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

   The **Private Zones** page is displayed.

4. Click in the upper left corner and select the desired region and project.
5. Click **Create Private Zone**. In the displayed dialog box, set the zone name to **ecs01**.
6. Click **OK**.

   View the created private zone on the **Private Zones** page.
7. Click the zone name.

   The **Record Sets** page is displayed.
8. Click **Add Record Set**.

   Add an A record set in the **ecs01** zone.
   - Set **Type** to **A – Map domains to IPv4 addresses**.
   - Leave the **Name** parameter blank.
   - Set **Value** to the private IP address of the ECS, for example, **192.168.1.10**.
9. Click **OK**.

   After the record set is created, 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 Configure a PTR Record to Map the IP Address of an ECS to a Domain Name?

PTR records enable users to query domain names based on IP addresses.

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

To map the EIP of the ECS to a domain name, refer to **Creating a PTR Record**.

NOTE

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

For example, if the private IP address is 192.168.1.10, the domain name in the PTR record must be **10.1.168.192.in-addr.arpa**.

In this case, you must create a private zone named **192.in-addr.arpa** and add a PTR record with its value set to **10.1.168.192.in-addr.arpa**.

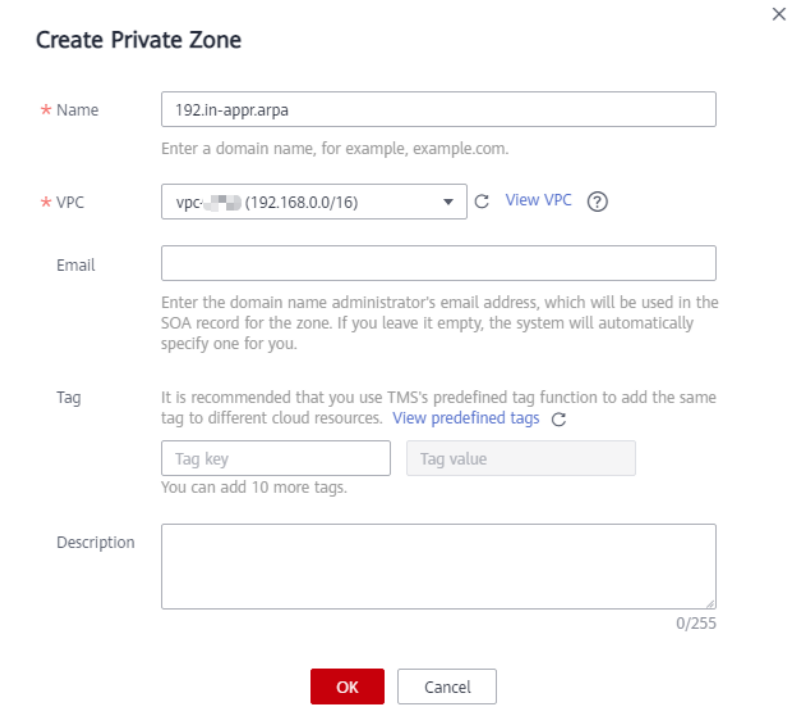
Creating a Private Zone

1. Log in to the management console.
2. Hover the cursor over in the upper left corner. In the service list, choose **Networking** > **Domain Name Service**.

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

   The **Private Zones** page is displayed.
4. Click in the upper left corner and select the desired region and project.
5. Click **Create Private Zone**.

Figure 5-1 Create Private Zone



6. Configure the parameters based on **Table 5-2**.

Table 5-2 Parameters for creating a private zone

Parameter	Description	Example Value
Name	Domain name Set the domain name suffix to **in-addr.arpa**.	192.in-addr.arpa
VPC	VPC to be associated with the private zone Select the VPC you want to associate with the private zone.	N/A

Parameter	Description	Example Value
Email	(Optional) Email address of the administrator managing the private zone. Recommended email address: **HOSTMASTER@*Domain name*** For more information about the email address, see **Why Was the Email Address Format Changed in the SOA Record?**	HOSTMASTER@example.com
Tag	(Optional) Identifier of a resource Each tag contains a key and a value. You can add a maximum of 10 tags to a zone. For details about tag key and value requirements, see **Table 5-3**.	example_key1 example_value1
Description	(Optional) Supplementary information about the zone You can enter a maximum of 255 characters.	This is a private zone.

Table 5-3 Tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 characters. • Cannot start or end with a space or contain special characters =*<>\,|/	example_key1

Parameter	Requirements	Example Value
Value	• Cannot be left blank. • Can contain a maximum of 43 characters. • Cannot start or end with a space or contain special characters =*<>\,|/	example_value1

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

   View the created private zone.

   NOTE

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

   - The SOA record set defines the DNS server that is the authoritative information source for a particular domain name.
   - The NS record set defines authoritative DNS servers for a domain name.

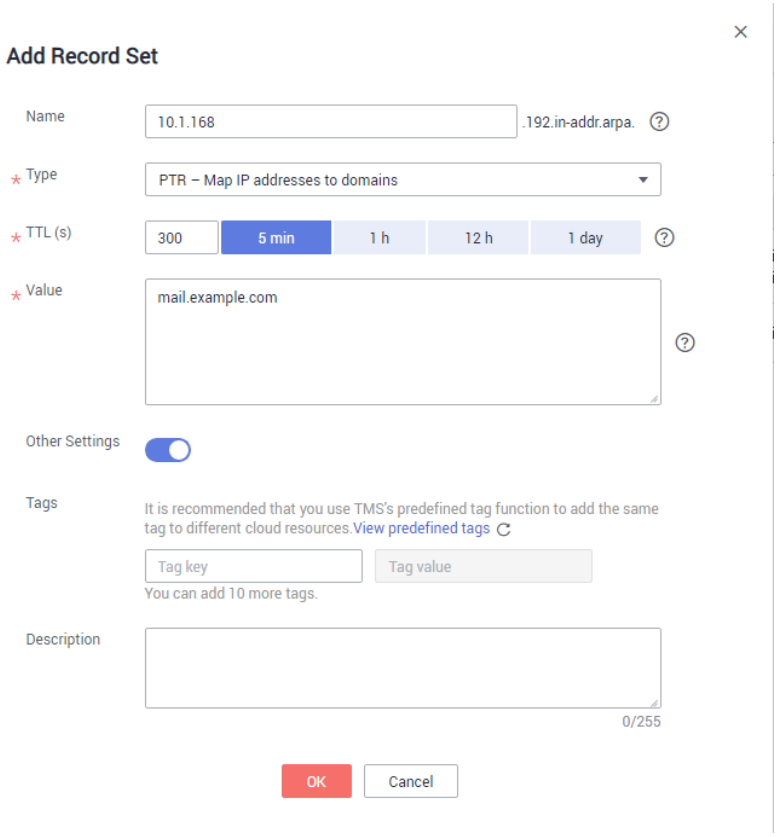
Adding a PTR Record

1. On the **Private Zones** page, click the name of the private zone that you have created.

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

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

Figure 5-2 Adding an A record set



3. Configure the parameters based on **Table 5-4**.

Table 5-4 Parameters for adding a PTR record

Parameter	Description	Example Value
Name	IP address in the PTR record (typed in reverse order).	10.1.168 For example, if the IP address is **192.168.1.10**, the domain name in the PTR record is **10.1.168.192.in-addr.arpa**. • If the private zone name is **192.in-addr.arpa**, enter **10.1.168** in the box. • If the private zone name is **1.168.192.in-addr.arpa**, enter **10** in the box.
Type	Type of the record set.	PTR – Map IP addresses to domains

Parameter	Description	Example Value
TTL (s)	Cache duration of the record set, in seconds.	The default value is 300s, which is, 5 minutes.
Value	Domain name mapped to the IP address. You can enter only one name.	mail.example.com
Tag	(Optional) Identifier of the PTR record. Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. This parameter is displayed when you expand **More Settings**. For details about tag key and value requirements, see **Table 5-3**.	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.

4. Click **OK**.
5. Switch back to the **Record Sets** page.

   View the added record set in the record set list of the zone and ensure that the status of the record set is **Normal**.

5.5 How Do I Configure a Public Domain Name and a Private Domain Name for My Website?

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

Private DNS servers translate domain names in VPCs and forward DNS queries for public domain names to public DNS servers. The following is an example that shows how an ECS accesses a website using a domain name.

- If the domain name is a private domain name you customize on the DNS console or is the domain name of a Huawei Cloud service, the private DNS server directly returns the resolution result.
- If the domain name has been registered with a domain name registrar, the private DNS server forwards the request to a public DNS server (for example, DNS server 114.114.114.114) and then returns the resolution result 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 result is

found, the private DNS server will return a message indicating that no record is found and will not forward the request to the public DNS server.

To resolve this issue, 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 123.example.com and configure record sets for it. 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 one or more VPCs in the same region.

If a private zone is associated with multiple VPCs, the private domain name takes effect in all the associated VPCs but cannot be used across them. However, if two VPCs are connected over a **VPC peering connection**, private domain names can be used across the two VPCs.

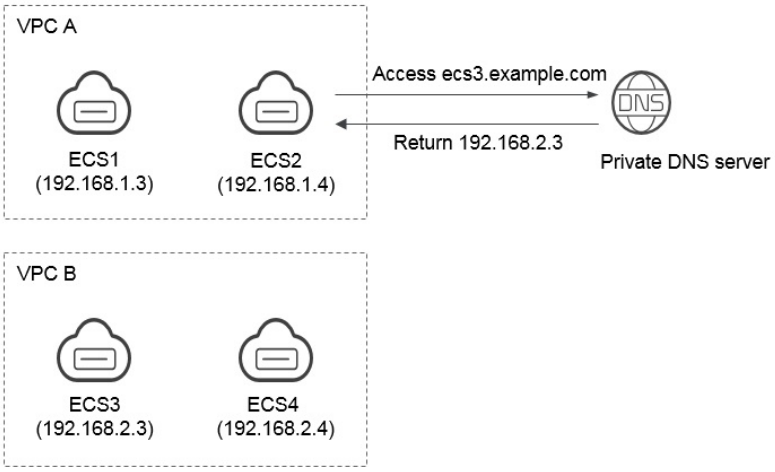
In the following example, a private zone is created for domain name **example.com**, and it has two VPCs associated and two record sets.

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

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 take effect only in associated VPCs. Therefore, 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?

Deleted VPCs will not be automatically disassociated from the private zones. If you delete a VPC 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 for all users 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, the private DNS servers will limit traffic issued from a single source IP address to 2,000 QPS. If a server initiates DNS query requests with an overwhelmingly high frequency, significantly in excess of normal service demands, and the QPS reaches 2,000, the additional requests will not be processed.

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

6 Reverse Resolution

6.1 What Is a PTR Resolution?

Generally, DNS is to resolve a domain name to an IP address. When you access a website domain name, DNS maps the domain name to the IP address of the website, so you can access the website content.

Reverse resolution obtains domain names or host addresses based on IP addresses. It is usually used in scenarios such as anti-spam and logging.

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

An A record is stored under a zone. Reverse resolution is to add the reverse top-level domain **.in-addr.arpa**. For example, the PTR record of IP address 192.0.2.255 is stored in 255.2.0.192.in-addr.arpa.

By default, a reverse domain name in the format of **ecs-x-x-x-x.compute.hwclouds-dns.com** is added to Huawei Cloud EIP. Resolve the PTR record of the EIP to obtain the default reverse domain name. You can also log in to the DNS console, choose **PTR Records**, and add a PTR record for the EIP. Then the default value will be overwritten.

7 Domain Transfer

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

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= ***Type*****]** ***Domain name Authoritative DNS server***
   - For Linux OS

     dig ***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.

   Typically, changes to DNS server addresses are quickly updated to top-level DNS servers and take effect on the Internet. However, some DNS service providers usually set the TTL value of the NS record to 48 hours. In this case, if the NS record is cached, the change will 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 change takes 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	This issue is the ninth official release, which incorporates the following changes: • Added **How Do I View and Change the DNS Address of a Domain Name?**. • Modified **What Is a PTR Resolution?**.
2020-06-17	This issue is the eighth official release, which incorporates the following changes: • Classified FAQs. • Added the following section: – **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: – 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	This issue is the seventh official release, which incorporates the following changes: Added new DNS addresses in **What Are DNS Server Addresses Provided by Huawei Cloud DNS?**
2020-02-12	This issue is the sixth official release, which incorporates the following changes: • Added examples in **How Do I Check Whether Record Sets Have 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	This issue is the fifth official release, which incorporates the following changes: Added the private DNS server addresses of the LA-Santiago region in **What Are the Private DNS Server Addresses Provided by Huawei Cloud?** Added the following content: • **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 Servers on Another Cloud?** • **Does DNS Support Explicit and Implicit URLs?** • **Why Can't I Access the Website Even Though the Domain Name Has Been Resolved Successfully?** • **What Are the Differences Between Public and Private Domain Names?** • **How Do I Configure a Public Domain Name and a Private Domain Name for My Website?** • **Can I Use Private Domain Names Across Regions?** • **How Do I Add Record Sets to Subdomains?** • **Does DNS Support IPv6?**
2019-08-23	This issue is the fourth official release, which incorporates the following changes: Updated the private DNS server addresses in the AP-Singapore region in **What Are the Private DNS Server Addresses Provided by Huawei Cloud?**
2019-07-02	This issue is the third official release, which incorporates the following changes: Optimized the following FAQs: • **How Do I Change Default DNS Servers of an ECS to Private DNS Servers Provided by the DNS Service?** • **What Is TTL?** • **What Are the Restrictions on Concurrent Private DNS Requests?**
2019-03-05	This issue is the second official release, which incorporates the following changes: • Updated the screenshots. • Added DNS server addresses in different regions in **What Are the Private DNS Server Addresses Provided by Huawei Cloud?**
2018-11-22	This issue is the first official release.

