Domain Name Service

Best Practices

Issue	01
Date	2025-02-28

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Configuring ISP Routing and Geolocation Routing

Scenarios

If end users access a domain name, DNS servers return the same IP address to them regardless of their carriers or geographical locations. This would increase network latency and affect user experience.

With configurable resolution lines, you can specify different IP addresses for the same domain name based on the carriers or geographical locations of end users.

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

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

This best practice describes how to configure ISP routing and geolocation routing for different end users.

- **Cross-carrier access in the Chinese mainland**: Configure a resolution line to return the most appropriate IP address used by each carrier to end users for nearby access.
- **Intelligent access around the globe**: Configure a region line to return the corresponding IP address based on the geographical locations of end users to quickly respond to user requests.

Example Lines

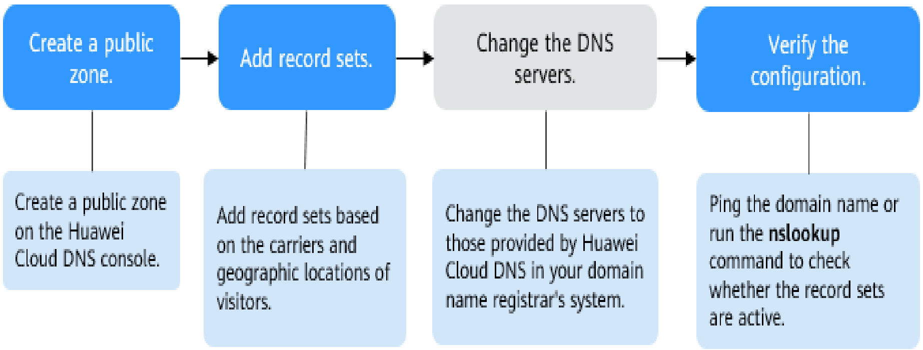
- **Returning IP addresses based on users' carriers**
  - China Unicom: 1.1.xx.xx
  - China Mobile: 2.2.xx.xx
  - China Telecom: 3.3.xx.xx
  - Other (such as CERNET, China Mobile Tietong, and Dr. Peng): 4.4.xx.xx
- **Returning IP addresses based on users' geographical locations (excluding Chinese mainland users)**

- Hong Kong, China: 5.5.xx.xx
- Macao, China: 6.6.xx.xx
- Taiwan, China: 7.7.xx.xx
- Europe, North America, South America, Africa, Oceania, Antarctica, and Abroad: 8.8.xx.xx

Process Flow

Figure 1-1 shows the process of configuring ISP lines and region lines.

Figure 1-1 Process of configuring ISP lines and region lines


Create a public zone.
Add record sets.
Change the DNS servers.
Verify the configuration.
Create a public zone on the Huawei Cloud DNS console.
Add record sets based on the carriers and geographic locations of visitors.
Change the DNS servers to those provided by Huawei Cloud DNS in your domain name registrar's system.
Ping the domain name or run the **nslookup** command to check whether the record sets are active.

Step 1: Create a Public Zone

Create a public zone for your domain name, for example, huawei-example.com. For details, see **Creating a Public Zone**.

Step 2: Add Record Sets

1. Locate the created public zone and click **Manage Record Sets** in the **Operation** column.

   The record set list is displayed.

2. Click **Add Record Set** to configure record sets for a subdomain (test.huawei-example.com) of the domain name.
   - ISP lines: Add record sets based on **Table 1-1** to route visitors based on their carriers.

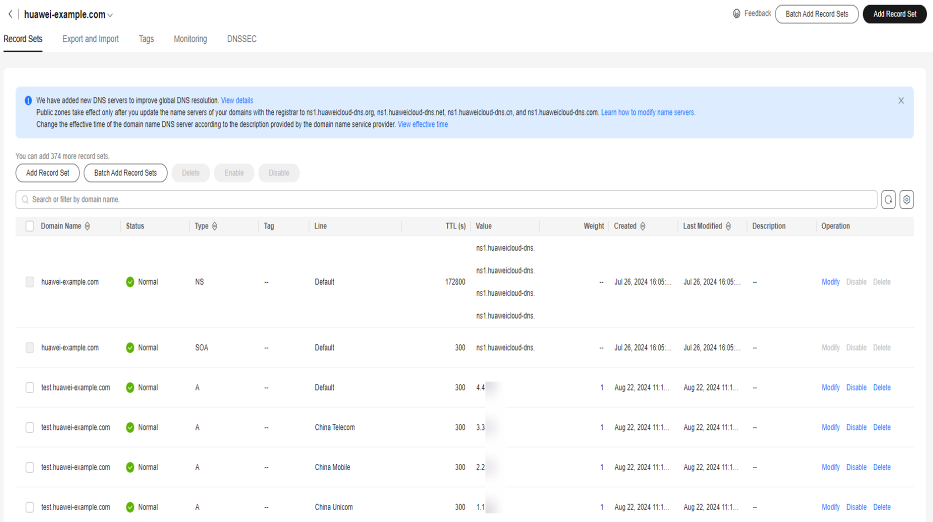
     Figure 1-2 displays all the configured ISP lines.

Table 1-1 ISP lines

Line Type	Carrier (IP Source of the Local DNS Egress of Visitors)	Record Set Value
ISP lines	China Unicom	1.1.xx.xx
	China Mobile	2.2.xx.xx
	China Telecom	3.3.xx.xx

Line Type	Carrier (IP Source of the Local DNS Egress of Visitors)	Record Set Value
Default	Other (such as CERNET, China Mobile Tietong, and Dr. Peng)	4.4.xx.xx

Figure 1-2 Record sets for ISP lines



We have added new DNS servers to improve global DNS resolution. View details
Public zones take effect only after you update the name servers of your domains with the registrar to ns1.huaweicloud-dns.org, ns1.huaweicloud-dns.net, ns1.huaweicloud-dns.cn, and ns1.huaweicloud-dns.com. Learn how to modify name servers.
Change the effective time of the domain name DNS server according to the description provided by the domain name service provider. View effective time

You can add 374 more record sets.

Domain Name	Status	Type	Tag	Line	TTL (s)	Value	Weight	Created	Last Modified	Description	Operation
huawei-example.com	Normal	NS	--	Default	172800	ns1.huaweicloud-dns. ns1.huaweicloud-dns. ns1.huaweicloud-dns. ns1.huaweicloud-dns.	--	Jul 26, 2024 16:05:...	Jul 26, 2024 16:05:...	--	Modify Disable Delete
huawei-example.com	Normal	SOA	--	Default	300	ns1.huaweicloud-dns.	--	Jul 26, 2024 16:05:...	Jul 26, 2024 16:05:...	--	Modify Disable Delete
test.huawei-example.com	Normal	A	--	Default	300	4.4	1	Aug 22, 2024 11:1...	Aug 22, 2024 11:1...	--	Modify Disable Delete
test.huawei-example.com	Normal	A	--	China Telecom	300	3.3	1	Aug 22, 2024 11:1...	Aug 22, 2024 11:1...	--	Modify Disable Delete
test.huawei-example.com	Normal	A	--	China Mobile	300	2.2	1	Aug 22, 2024 11:1...	Aug 22, 2024 11:1...	--	Modify Disable Delete
test.huawei-example.com	Normal	A	--	China Unicom	300	1.1	1	Aug 22, 2024 11:1...	Aug 22, 2024 11:1...	--	Modify Disable Delete

– Region lines: Add the record sets based on **Table 1-2** to route visitors based on their locations.

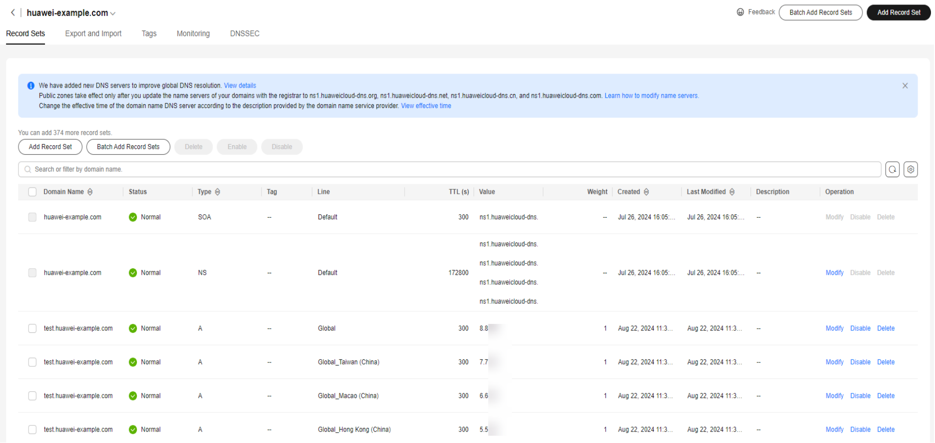
Figure 1-3 displays all the configured region lines.

Table 1-2 Region lines

Line Type	Geolocation (IP Source of the Local DNS Egress of Visitors)	Record Set Value
Asia Pacific	Hong Kong, China	5.5.xx.xx
	Macao, China	6.6.xx.xx
	Taiwan, China	7.7.xx.xx
Global-All regions	Other regions	8.8.xx.xx
North America-All regions		
South America-All regions		
Africa-All regions		
Oceania-All regions		

Line Type	Geolocation (IP Source of the Local DNS Egress of Visitors)	Record Set Value
Antarctica-All regions		
Abroad		

Figure 1-3 Record sets for region lines



< | huawei-example.com

Record Sets | Export and Import | Tags | Monitoring | DNSSEC

Feedback | Batch Add Record Sets | Add Record Set

We have added new DNS servers to improve global DNS resolution. View details
Public zones take effect only after you update the name servers of your domains with the registrar to ns1.huaweicloud-dns.org, ns1.huaweicloud-dns.net, ns1.huaweicloud-dns.cn, and ns1.huaweicloud-dns.com. Learn how to modify name servers.
Change the effective time of the domain name DNS server according to the description provided by the domain name service provider. View effective time

You can add 374 more record sets.

Add Record Set | Batch Add Record Sets | Delete | Enable | Disable

Search or filter by domain name.

Domain Name	Status	Type	Tag	Line	TTL (s)	Value	Weight	Created	Last Modified	Description	Operation
huawei-example.com	Normal	SOA	--	Default	300	ns1.huaweicloud-dns.	--	Jul 26, 2024 16:05:...	Jul 26, 2024 16:05:...	--	Modify Disable Delete
huawei-example.com	Normal	NS	--	Default	172800	ns1.huaweicloud-dns. ns1.huaweicloud-dns. ns1.huaweicloud-dns. ns1.huaweicloud-dns.	--	Jul 26, 2024 16:05:...	Jul 26, 2024 16:05:...	--	Modify Disable Delete
test.huawei-example.com	Normal	A	--	Global	300	8.8	1	Aug 22, 2024 11:3...	Aug 22, 2024 11:3...	--	Modify Disable Delete
test.huawei-example.com	Normal	A	--	Global_Taiwan (China)	300	7.7	1	Aug 22, 2024 11:3...	Aug 22, 2024 11:3...	--	Modify Disable Delete
test.huawei-example.com	Normal	A	--	Global_Macao (China)	300	6.6	1	Aug 22, 2024 11:3...	Aug 22, 2024 11:3...	--	Modify Disable Delete
test.huawei-example.com	Normal	A	--	Global_Hong Kong (China)	300	5.5	1	Aug 22, 2024 11:3...	Aug 22, 2024 11:3...	--	Modify Disable Delete

Step 3: Change the DNS Servers

The record sets you added in **Step 2: Add Record Sets** take effect only when Huawei Cloud DNS servers are used for domain name resolution.

For details, see **How Do I View and Change the DNS Servers of a Domain Name?**

NOTE

Generally, the changes to DNS servers will take effect within 48 hours, but the time may vary depending on the domain name registrar's cache duration.

Step 4: Check Whether the Record Sets Take Effect

For details, see **How Do I Check Whether Record Sets Have Taken Effect?**

Helpful Links

- **What Do I Do If a Record Set Does Not Take Effect?**
- **Why a Website Can't Be Accessed Even Though Its Domain Name Can Be Resolved?**
- **Why Can't My Website Be Accessed over HTTPS?**

2 Configuring Private Domain Names for ECSs for Smooth ECS Switchover

Overview

Scenario

If one of your ECSs is malfunctioning and you need to use the backup ECS, but you have not configured private domain names for the two ECSs, you have to change the private IP address in the code for the faulty ECS. This will interrupt your services, and you need to launch your website again.

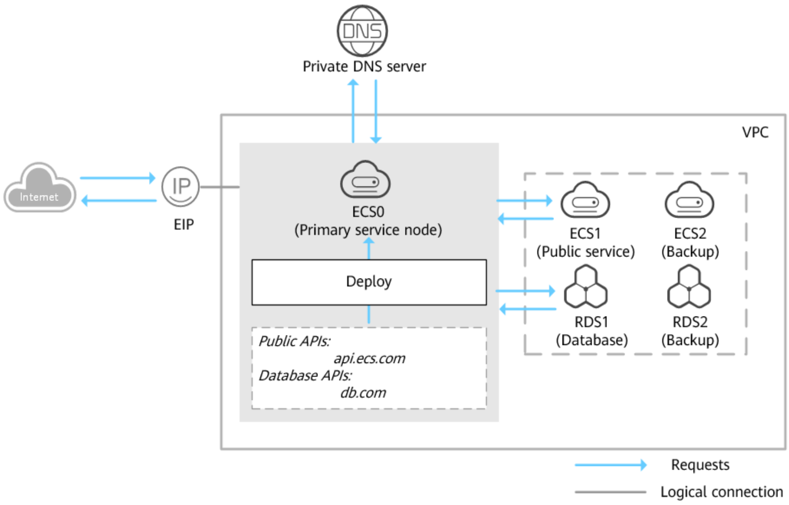
Here is the solution: Configure private domain names for the ECSs and include the private domain names in the code. If one ECS is malfunctioning, you only need to change the DNS record sets to direct traffic to a normal ECS. Your services will not be interrupted, and you do not need to launch the website again.

Architecture

Figure 2-1 shows the networking where ECSs and RDS instances are deployed in a VPC.

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

Figure 2-1 Networking example



Advantages

- **Higher efficiency and security**

  You can use private domain names to access ECSs in the VPCs, without going through the Internet.

- **Easier management**

  In code, domain names are easier to be modified than IP addresses. When ongoing services need to run on another ECS, you only need to change the DNS record sets without modifying the code.

Resource Planning

The following table lists the planned private zones and record sets.

Table 2-1 Private zones and record sets for each server

Resource	Private Zone	Associated VPC	Private IP Address	Record Set Type	Description
ECS1	api.ecs.com	VPC_001	192.168.2.8	A	Public service node
ECS2	api.ecs.com	VPC_001	192.168.3.8	A	Backup for the public service node
RDS1	db.com	VPC_001	192.168.2.5	A	Service database
RDS2	db.com	VPC_001	192.168.3.5	A	Backup database

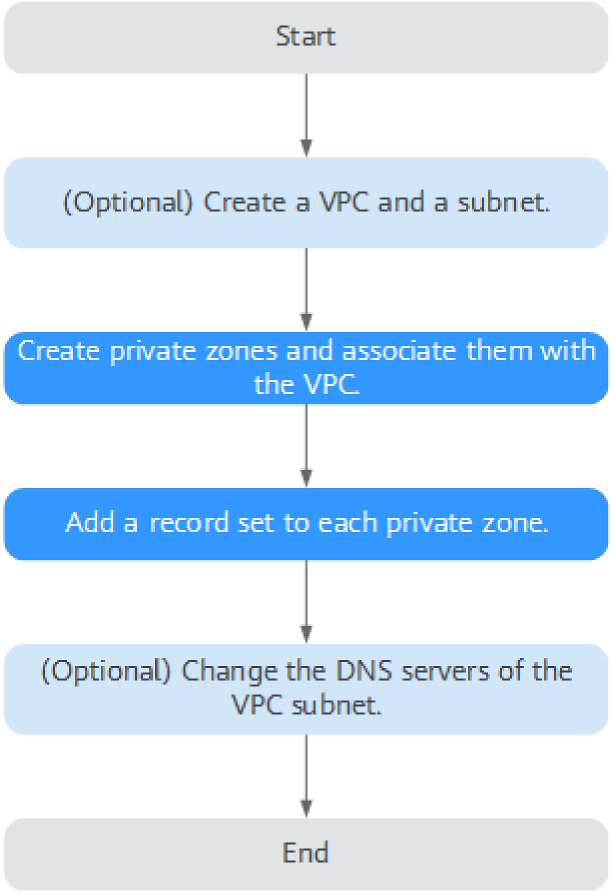
Table 2-2 Resource planning

Region	Service	Resource	Description	Quantity	Monthly Price
CN-Hong Kong	VPC	VPC_001	The DNS servers must be the same as the private DNS servers of Huawei Cloud. For details, see **What Are Huawei Cloud Private DNS Servers?**	1	Free
	ECS	ECS0 ECS1 ECS2	● Private domain name: api.ecs.com ● Associated VPC: VPC_001 ● ECS1: public service node Private IP address: 192.168.2.8 ● ECS2: backup service node ● Private IP address: 192.168.3.8	3	**ECS Product Pricing Details**
	RDS	RDS1 RDS2	● Private domain name: db.com ● Associated VPC: VPC_001 ● RDS1: service database Private IP address: 192.168.2.5 ● RDS2: backup database Private IP address: 192.168.3.5	2	**RDS Product Pricing Details**
	DNS	api.ces.com db.com	● api.ces.com Associated VPC: VPC_001 Record set type: A Value: 192.168.2.8 ● db.com Associated VPC: VPC_001 Record set type: A Value: 192.168.2.5	2	Free

Configuring Private Zones

Figure 2-2 shows the process for configuring private zones.

Figure 2-2 Process for configuring private zones


Start
(Optional) Create a VPC and a subnet.
Create private zones and associate them with the VPC.
Add a record set to each private zone.
(Optional) Change the DNS servers of the VPC subnet.
End

1. (Optional) On the VPC console, create a VPC and a subnet when you are configuring private domain names for servers during website deployment.
2. On the DNS console, create private zones and associate them with the VPC, and add a record set to each private zone.
3. (Optional) On the VPC console, change the DNS servers for the VPC subnet when you are configuring private domain names for servers.

Procedure

Step 1 (Optional) Create a VPC and a subnet.

Before configuring private domain names for the ECSs and databases required by your website, you need to create a VPC and a subnet.

1. Go to the **Create VPC** page.
2. Configure the parameters based on **Table 2-3**.

Table 2-3 Parameters for creating a VPC

Parameter	Description	Example Value
Region	Region of the VPC. For lower network latency and quicker resource access, select the nearest region.	CN-Hong Kong
Name	VPC name	VPC_001
CIDR Block	Network range of the VPC. All subnets must be within this range. Choose one from the following CIDR blocks: – 10.0.0.0/8–24 – 172.16.0.0/12–24 – 192.168.0.0/16–24	192.168.0.0/16
Name (default subnet)	Subnet name	Subnet
CIDR Block (default subnet)	Network range of the subnet, which must be within the VPC	192.168.0.0/24
Gateway	Gateway address of the subnet	192.168.0.1
DNS Server Address	Set the DNS servers for the VPC subnet to those provided by Huawei Cloud DNS.	100.125.1.250 100.125.3.250

3. Click **Create Now**.

Step 2 Create private zones.

Create private zones for the domain names used by ECS1 and RDS1.

1. Go to the **Private Zones** page.
2. Click **Create Private Zone**.
3. Configure the parameters based on **Table 2-4**.

Table 2-4 Parameters for creating a private zone

Parameter	Description	Example Value
Name	Private domain name. You can create custom any compliant domain names, even top-level ones.	api.ecs.com

Parameter	Description	Example Value
Recursive resolution proxy for subdomains	If you select this option, when you query subdomains that are not configured in the zone namespace, DNS will forward the DNS queries to the Internet for recursive resolution and use the result from authoritative DNS servers.	Enable it.
Region	Region of the VPC associated with the private zone.	CN-Hong Kong
VPC	VPC to be associated with the private zone	VPC_001
Tag	(Optional) Identifier used to group and search for resources. A tag consists of a key and value. You can set tags when there are many zones in your account. For details about tag key and value requirements, see **Table 2-5**.	N/A
Description	(Optional) Description of a zone. You can enter a maximum of 255 characters.	This is a private zone.

Table 2-5 Tag key and value requirements

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

4. Click **OK**.

   A private zone is created for api.ecs.com.

   You can view details about this private zone on the **Private Zones** page.

NOTE

If you click **Manage Record Sets** in the **Operation** column, you can see that record sets of the SOA type and NS type have been created in the zone.

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

5. Repeat steps **3** to **5** to create a private zone for db.com.

   For details about private domain names, see **Table 2-1**.

Step 3 Add a record set to each private zone.

Add record sets to translate private domain names to private IP addresses of ECS1 and RDS1.

1. Click the domain name.

   The record set page is displayed.
2. Click **Add Record Set**.
3. Configure the parameters based on **Table 2-6**.

Table 2-6 Parameters for adding an A record set

Parameter	Description	Example Value
Name	Domain name prefix If this parameter is left blank, the primary domain name, for example, api.ecs.com, will be resolved	N/A
Type	Type of the record set	A – Map domains to IPv4 addresses
TTL (s)	Caching period of the record set on a DNS server If your service address is frequently changed, set TTL to a small value.	Default value: 300s
Value	IPv4 addresses mapped to the domain name. Every two IPv4 addresses are separated using a line break. Enter the private IP address of the ECS, for example, ECS1.	192.168.2.8

Parameter	Description	Example Value
Tag	(Optional) Identifier used to group and search for resources. A tag consists of a key and value. You can set tags when there are many record sets in your account. For details about tag key and value requirements, see **Table 2-5**.	N/A
Description	(Optional) Description of the record set	N/A

4. Click **OK**.

   An A record set is added for api.ecs.com.

5. Repeat steps **3.1** to **3.4** to add an A record set for db.com.

   Set the record set value of **db.com** to **192.168.2.5**.

   For details, see **Table 2-2**.

Step 4 (Optional) Change the DNS servers for the VPC subnet.

After you configure private domain names for nodes in the website application, you need to change the DNS servers of the VPC subnet to those provided by the DNS service so that the domain names can be resolved.

For details, see **How Do I Change Default DNS Servers of an ECS to Huawei Cloud Private DNS Servers?**

Step 5 Switch to the backup ECS.

When ECS1 becomes faulty, you can switch services to ECS2 by changing the value of the record set added to private zone **api.ecs.com**.

1. Log in to the management console.
2. Click 📍 in the upper left and select **CN-Hong Kong**.
3. Choose **Networking** > **Domain Name Service**.

   The DNS console is displayed.

4. In the navigation pane on the left, choose **Private Zones**.
5. In the private zone list, click the domain name (api.ecs.com) of the zone.
6. Locate the A record set and click **Modify** under **Operation**.
7. Change the value to **192.168.3.8**.
8. Click **OK**.

Traffic to ECS1 will be directed to ECS2 by the private DNS server.

----End

3 Setting CAA Records to Prevent CAs from Issuing Unauthorized HTTPS Certificate

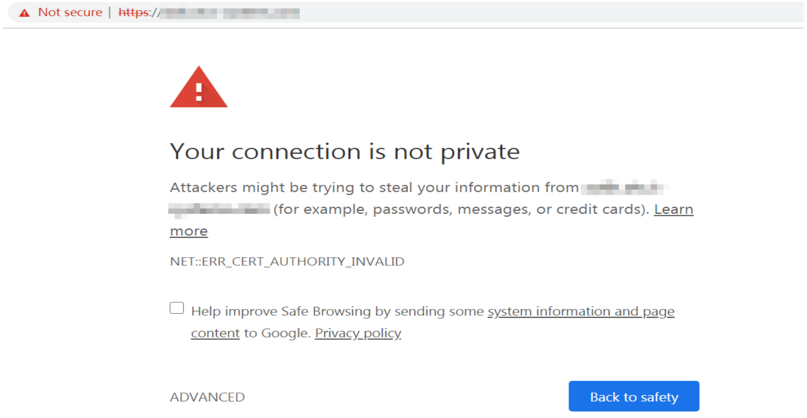
Overview

Scenarios

Certification Authority Authorization (CAA) is a way to ensure that HTTPS certificates are issued by authorized certificate authorities (CAs). CAA complies with IETF RFC 6844 requirements. Since September 8, 2017, all CAs must check CAA record sets before issuing a certificate.

There are hundreds of CAs in the world that can issue HTTPS certificates for websites. If a CA is blacklisted, the browser will no longer trust the HTTPS certificates issued by this CA. If you try to access websites that have those certificates, the browser will prompt that the websites are not secure.

Figure 3-1 Untrusted HTTPS certificate warning



Not secure | ~~https~~://[redacted]

Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

According to the CAA standards, a compliant CA must check CAA record sets of a domain name before issuing certificates.

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

Other CAs can also issue certificates for this domain name, but may issue unauthorized certificates.

- 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 that does not authorize it to issue certificates, the CA will not issue HTTPS certificates for the domain name to avoid unauthorized HTTPS certificates.

Using Huawei Cloud DNS, you can configure CAA record sets for your public domain names on the DNS console.

Advantage

Configuring CAA record sets for website domain names enables you to configure a CA whitelist. Only authorized CAs can issue certificates for your website.

Notes and Constraints

A CAA record set consists of a flag byte and a tag-value pair in the format of **[flag] [tag] [value]**.

- **flag**: CA identifier, an unsigned character ranging from 0 to 255. Usually, it is specified to **0**.
- **tag**: You can enter 1 to 15 characters. Only letters and digits from 0 to 9 are allowed. The tag can be one of the following:
  - **issue**: authorizes the CA to issue all types of certificates.
  - **issuewild**: authorizes the CA to issue wildcard certificates.
  - **iodef**: requests notifications once a CA receives invalid certificate requests.
- **value**: authorized CA or email address/URL required for notifications once the CA receives invalid certificate requests. The value depends on the setting of the tag and must be enclosed in quotation marks (""). The value can contain no more than 255 characters. Only letters, digits, spaces, and special characters -#*?&_~=:;.@+^/!% are allowed.

You can set CAA record sets based on the following rules to suit different scenarios.

Table 3-1 Configuration of CAA record sets

Function	Example Value	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**). The 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**).

Function	Example Value	Description
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/"	The 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"	A CAA record set is configured for **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. ● If a violation occurs, the CA sends a notification to **admin@domain.com**.

Resource and Cost Planning

The following tables list the planned public zone and record set.

Table 3-2 Domain name

Service	Public Zone	Record Set Type
DNS	domain.com	CAA

Table 3-3 Required resources and their prices

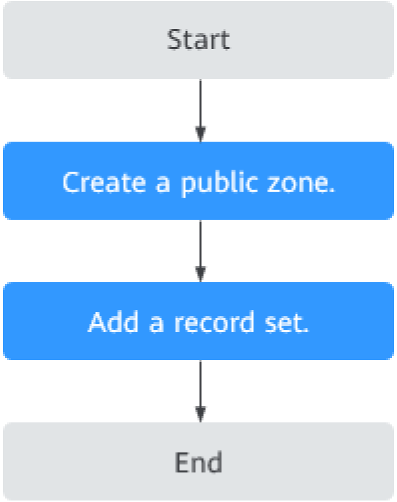
Service	Resource	Description	Quantity	Monthly Price
Domains	Domain name	Public domain name: domain.com	1	N/A

Service	Resource	Description	Quantity	Monthly Price
DNS	- Public zone - Record set	- Public domain name: domain.com: - Record set type: CAA Value: 0 issue "ca.abc.com" 0 iodef "mailto:admin@domain.com"	1	Free

Adding a CAA Record Set to a Public Zone

Figure 3-2 shows the process for adding a CAA record set to a public zone.

Figure 3-2 Adding a CAA record set to a public zone



Procedure

Step 1 Create a public zone.

1. Go to the **Public Zones** page.
2. Click **Create Public Zone**.
3. Configure the parameters based on **Table 3-4**.

Table 3-4 Parameters for creating a public zone

Parameter	Description	Example Value
Domain Name	Name of the public zone, which is the domain name you have registered with a domain name registrar For details about the domain name format, see **Domain Name Format and DNS Hierarchy**.	domain.com
Email	(Optional) Email address of the administrator managing the domain name. It is recommended that you set the email address to **HOSTMASTER@***Domain name*. For more information about the email address, see **Why Was the Email Address Format Changed in the SOA Record?**	N/A
Tag	(Optional) Identifier of the zone. Each tag contains a key and a value. You can add up to 20 tags to a zone.	example_key1 example_value1
Description	(Optional) Supplementary information about the zone The description can contain no more than 255 characters.	This is a zone example.

4. Click **OK**.

Step 2 Add a CAA record set.

1. In the public zone list, click the domain name **domain.com**.

   The **Record Sets** tab is displayed.

2. Click **Add Record Set**.

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

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

Table 3-5 Parameters for adding a CAA record set

Parameter	Description	Example Value
Name	Prefix of the domain name to be resolved. For example, if the domain name is domain.com, the domain name prefix can be any of the following: – **www**: The domain name is www.domain.com, which is used for a website. – Left blank: The domain name is domain.com. To use an at sign (@) as the domain name prefix, just leave this parameter blank. – **abc**: The domain name to be resolved is abc.domain.com. – **mail**: The domain name to be resolved is mail.domain.com, which is used for email servers. – *****: The domain name is *.domain.com, which is a wildcard domain name, covering all subdomains of domain.com.	Left blank
Type	Type of the record set A message may be displayed, indicating that the record set you are trying to add conflicts with an existing record set of the zone. For details, see **Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?**	CAA – Grant certificate issuing permissions to CAs

Parameter	Description	Example Value
Line	Resolution line. The DNS server uses information about end users' carrier networks or geographical locations to determine the most appropriate server IP address to return. The default value is **Default**. This parameter is only configurable for public zone record sets. – **Default**: returns the default resolution result when no resolution line is set based on end users' carrier networks or geographical locations. – **ISP**: returns the resolution result based on end users' carrier networks. – **Region**: returns the resolution result based on end users' geographical locations.	Default
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The value ranges from **1** to **2147483647**, and the default value is **300**. If your service address changes frequently, set TTL to a smaller value. Learn more about **TTL**.	300

Parameter	Description	Example Value
Value	CA to be authorized to issue certificates for a domain name or its subdomains. You can enter up to 50 different IP addresses, each on a separate line. The format is *[flag] [tag] [value]*. Configuration rules: – **flag**: CA identifier, an unsigned character ranging from 0 to 255. Usually, it is specified to **0**. – **tag**: You can enter 1 to 15 characters. Only letters and digits from 0 to 9 are allowed. The tag can be one of the following: ■ **issue**: authorizes the CA to issue all types of certificates. ■ **issuewild**: authorizes the CA to issue wildcard certificates. ■ **iodef**: requests notifications once a CA receives invalid certificate requests. – **value**: authorized CA or email address/URL required for notification once the CA receives invalid certificate requests. The value depends on the value of **tag** and must be enclosed in quotation marks (""). The value can contain no more than 255 characters. Only letters, digits, spaces, and special characters -#*?&_~=:;.@+^/!% are allowed.	0 issue "ca.abc.com" 0 iodef "mailto:admin@domain.com"
Weight	(Optional) Weight for the record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only configurable for public zone record sets. If a resolution line in a zone contains multiple record sets of the same type, you can set different weights to each record set.	1

Parameter	Description	Example Value
Tag	(Optional) Identifier of the record set. Each tag contains a key and a value. You can add up to 20 tags to a record set.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set. The description can contain no more than 255 characters.	The description of the hostname.

4. Click **OK**.

----End

Checking Whether the 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:

```
dig caa www.domain.com +trace
```