Domain Name Service

Best Practices

Issue 01

Date 2018-11-21



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Setting CAA Records to Prevent Unauthorized HTTPS Certificate Issuing..... 1
2 Configuring a Private Domain Name for an ECS..... 5

 Copyright © Huawei Technologies Co., Ltd.

1 Setting CAA Records to Prevent Unauthorized HTTPS Certificate Issuing

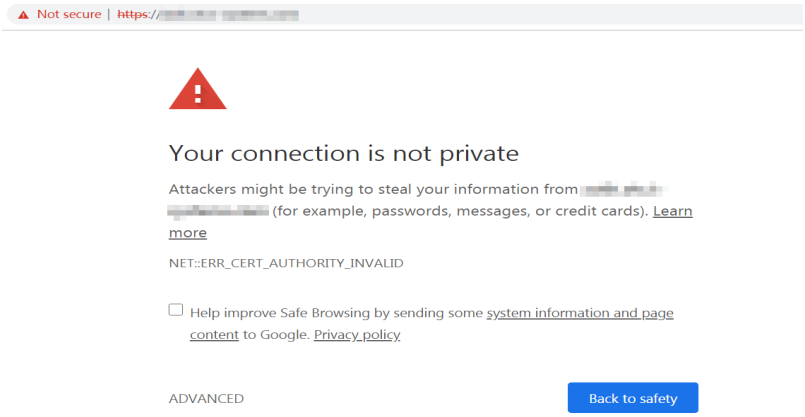
Certification Authority Authorization (CAA) is a way to ensure that HTTPS certificates are issued by authorized certificate authorities (CAs). It is in compliance with IETF RFC 6844 standards. Since September 8, 2017, all CAs are required to check CAA records before issuing a certificate.

Using HUAWEI CLOUD DNS, you can add CAA records for your public domain names on the web-based management console.

Background

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 users try to access websites installed with those certificates, the browser will prompt that the websites are not secure.

Figure 1-1 Untrusted HTTPS certificate warning



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

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

 Copyright © Huawei Technologies Co., Ltd.

Any other CAs are also able to issue certificates for this domain name, bringing risks of certificate mis-issuing.

- 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 HTTPS certificates for the domain name. In this case, HTTPS certificates will not be mis-issued.

Adding CAA records for website domain names enables you to configure a CA whitelist. Only authorized CAs can issue certificates for your websites, improving network security.

Configuration Rule

A CAA record consists of a flags bytes and a tag-value pair. It is formatted as **[flag] [tag] [value]**.

The elements in a CAA record are described as follows:

- **flag**: CA identifier, which is an unsigned character ranging from 0 to 255. Usually, it is specified to **0**.
- **tag**: a string of 1 to 15 characters composed of upper- and lower-case letters and digits from 0 to 9. The tag can be the following:
  - **issue**: authorizes CAs to issue all types of certificates.
  - **issuewild**: authorizes CAs to issue wildcard certificates.
  - **iodef**: requests notifications once CAs receive invalid certificate requests.
- **value**: authorized CA or email address/URL for notifications once the CA receives invalid certificate requests, depending on the setting of the tag. The value must be enclosed in quotation marks (""). It is a string of 1 to 255 characters, including letters, digits, spaces, and special characters -#*?&_~=:;.@+^/!%

You can set CAA records based on the following rules in different scenarios.

Table 1-1 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	0 iodef "mailto:admin@domain.com"	When a certificate issuing request violates the CAA record, the CA will notify the domain name holder of the violation.

 Copyright © Huawei Technologies Co., Ltd.

Function	Example	Description
the domain name holder.	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.
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**.

Adding a CAA Record Set

1. Log in to the management console.
2. In the **Network** category, click **Domain Name Service**.
   The DNS console is displayed.
3. In the navigation pane, choose **DNS Resolution** > **Public Zones**.
   The **Public Zones** page is displayed.
4. In the public zone list, click the zone name **domain.com**.
   The record set page is displayed.
5. Click **Add Record Set**.
   The **Add Record Set** box is displayed.
6. Set CAA record set parameters.
   - **Type**: **CAA – Grant certificate issuing permissions to CAs**
   - **Line**: **Default**
   - **TTL**: **300s** (5 minutes)
   - **Value**:
     0 issue "ca.abc.com"
     0 iodef "mailto:admin@domain.com"
7. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Checking Whether a CAA Record Takes Effect

You can run the **dig** command to check whether the CAA record has taken effect.

The command format is: **dig** [Type] [Domain name] **+trace**.

For example:

dig caa www.example.com +trace

NOTE

If the OS does not support the **dig** command, you need to manually install it first.

 Copyright © Huawei Technologies Co., Ltd.

2 Configuring a Private Domain Name for an ECS

Background

Private domain names do not need registration and take effect only within VPCs. They are resolved by private DNS servers. With private domain names, you can have your own authoritative DNS servers in VPCs and avoid exposing your DNS records to the Internet, improving resolution efficiency, reducing latency, and preventing DNS spoofing.

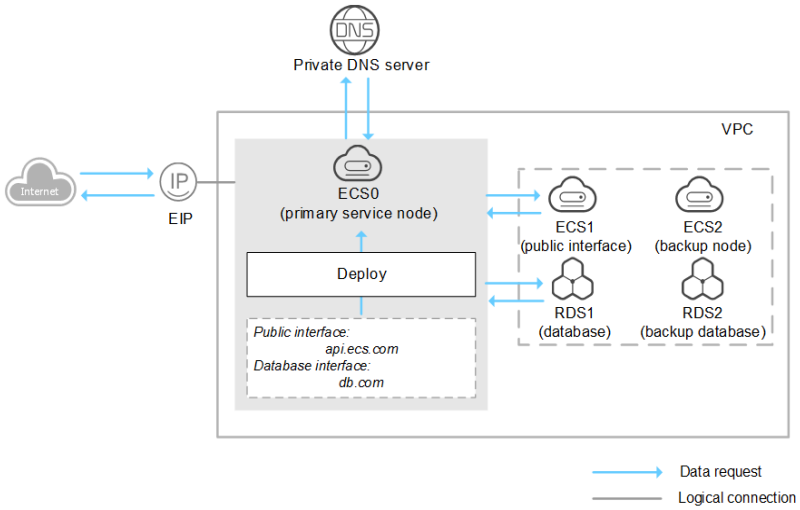
By creating private domain names for ECSs in VPCs, you can:

- Access ECSs in the VPCs through private domain names without going through the Internet, achieving higher efficiency and security.
- Write domain names, instead of IP addresses in the code. When an ECS is changed, you only need to change the DNS records without modifying the code.

Application Scenario

Figure 2-1 shows a typical application scenario of private domain names.

Figure 2-1 Networking example



 Copyright © Huawei Technologies Co., Ltd.

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

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

In the network, after ECS1 becomes faulty, services on it need to be switched to ECS2 (the backup). However, if no private domain name is configured for the ECSs, you need to change the private IP address in the code deployed on ECS0. Such change will interrupt services, and you must publish the website again.

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

This guide describes how to configure private domain names for cloud servers.

Data Planning

Table 2-1 lists the private domain names planned for the cloud servers.

Table 2-1 Private domain name planning

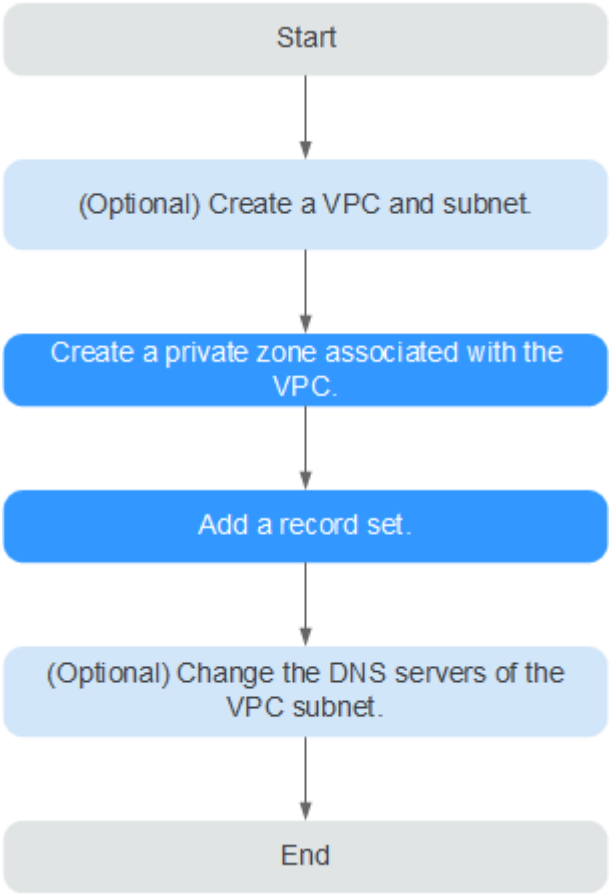
Item	Domain Name	Associated VPC	Private IP Address	Record Set Type	Description
ECS1	api.ecs.com	VPC_001	192.168.2.8	A	Public service interface
ECS2	api.ecs.com	VPC_001	192.168.3.8	A	Backup for the public service interface
RDS1	db.com	VPC_001	192.168.2.5	A	Service database
RDS2	db.com	VPC_001	192.168.3.5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

Operation Procedure

Figure 2-2 shows the process to configure private domain names.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 Process to configure private domain names



Process description:

- "Create a VPC and subnet" is performed on the VPC console. This operation is required only when you are configuring private domain names for servers during initial website deployment.
- "Create a private zone associated with the VPC" and "Create a record set" are performed on the DNS console.
- "Change the DNS servers of the VPC subnet" is performed on the VPC console. This operation is required only when you are configuring private domain names for servers on which your website services are already running.

(Optional) Create a VPC and Subnet

Before configuring private domain names for ECSs and database nodes during website deployment, you need to create a VPC and subnet.

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. In the **Network** category, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Virtual Private Cloud**.
5. Click **Create VPC** and set parameters based on **Table 2-2**.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-2 VPC parameter description

Parameter	Description	Example Value
Region	Region of the VPC. For low network latency and quick resource access, select the nearest region.	CN North-Beijing1
Name	VPC name	VPC_001
CIDR Block	Network range of the VPC. All VPC subnets must be within this range. The following CIDR blocks are supported: • 10.0.0.0/8–24 • 172.16.0.0/12–24 • 192.168.0.0/16–24	192.168.0.0/16
Name (Subnet Settings)	Subnet name	Subnet
CIDR Block (Subnet Settings)	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 severs of the VPC subnet to those provided by HUAWEI CLOUD DNS.	100.125.1.250 100.125.21.250

6. Click **Create Now**.

Create a Private Zone

Create private zones for the domain names of ECS1 and RDS1.

1. In the **Network** category, click **Domain Name Service**.
   The DNS console is displayed.
2. In the navigation pane, Choose **DNS Resolution** > **Private Zones**.
3. Click **Create Private Zone**.
4. Configure the parameters according to **Table 2-3**.

Table 2-3 Parameters required for creating a private zone

Parameter	Description	Example Value
Name	Private domain name. You can customize any correctly formatted domain names, even top-level ones.	api.ecs.com

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
VPC	VPC to be associated with the private zone	VPC_001
Email	(Optional) Email address of the administrator managing the private zone. It is recommended that you set the email address to **HOSTMASTER@Domain name**. For more details about the email address, see **Why Is the Email Address Format Changed in the SOA Record?**	HOSTMASTER@ecs1.com
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 2-4**.	-
Description	(Optional) Description of a zone. The value cannot exceed 255 characters.	This is a private zone.

Table 2-4 Tag key and value requirements

Parameter	Requirement	Example Value
Key	• Cannot be left blank. • Must be unique for each resource. • Consists of at most 36 characters. • Cannot start or end with a space or contain =*<>\,|/ and Unicode characters.	example_key1
Value	• Cannot be left blank. • Consists of at most 43 characters. • Cannot start or end with a space or contain =*<>\,|/ and Unicode characters.	example_value1

5. Click **OK**. A private zone **api.ecs.com** is created.

   You can query information about the private zone you created on the **Private Zones** page.

Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> Click the zone name to query detailed zone information. The system has created record sets of the SOA type and NS type in the zone.
>
> - The SOA record set determines the DNS server that is the authoritative information source for a particular domain name.
> - The NS record set defines authoritative DNS servers for a zone.

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

   For details about domain name planning, see **Table 2-1**.

Create a Record Set

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

1. In the zone list on the **Private Zones** page, click the name of the private zone you created.

   The record set page is displayed.
2. Click **Add Record Set**.
3. Configure the parameters according to **Table 2-5**.

Table 2-5 Parameters required for adding a record set of the A type

Parameter	Description	Example Value
Name	Domain name prefix If this parameter is left blank, the record set name is **api.ecs.com** by default.	-
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.	The default value is 300s, that is, **5 min**.
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.	192.168.2.8

Copyright © Huawei Technologies Co., Ltd.

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 2-4**.	-
Description	(Optional) Description of the record set	-

4. Click **OK**. An A record set is added for **api.ecs.com**.
5. Repeat steps **1** to **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, check **Table 2-1**.

(Optional) Change the DNS Servers of 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 correctly resolved.

For details, see **How Do I Switch to a Private DNS Server?**

Switch to the Backup ECS

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

1. Log in to the management console.
2. Click  in the upper left and select **CN North-Beijing1**.
3. In the **Network** category, click **Domain Name Service**.
   The DNS console is displayed.
4. In the navigation pane, Choose **DNS Resolution** > **Private Zones**.
5. In the private zone list, click the name of the zone **api.ecs.com**.
6. Locate the A record set and click **Modify** under **Operation**.
7. Change the value to **192.168.3.8**.
8. Click **OK**. The record set is modified.

Traffic from ECS0 to ECS1 will be seamlessly directed to ECS2 by the private DNS server.

Copyright © Huawei Technologies Co., Ltd.