Domain Name Service

Best Practices

Issue	01
Date	2024-03-15

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

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

Trademarks and Permissions

HUAWEI 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

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

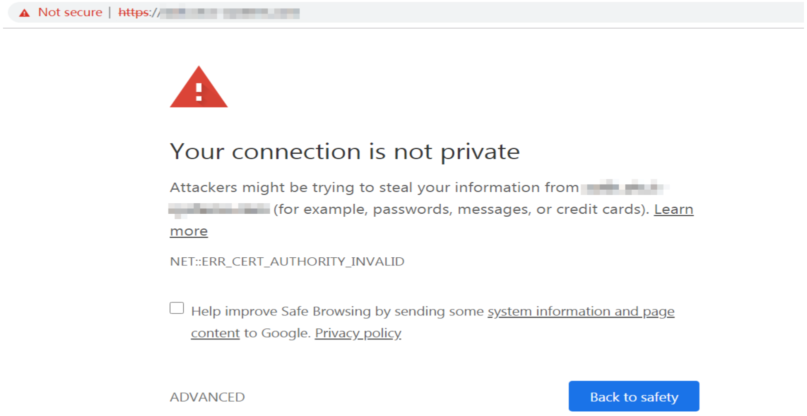
Overview

Scenario

Certification Authority Authorization (CAA) is a way to ensure that HTTPS certificates are issued by authorized certificate authorities (CAs). It complies with IETF RFC 6844 standards. 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 1-1 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 add CAA record sets for your public domain names on the management 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**: 1 to 15 characters, including letters and digits from 0 to 9. 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 the CA receives invalid certificate requests.
- **value**: authorized CA or email address/URL 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 up to 255 characters, consisting of letters, digits, spaces, and special characters - #*?&_~=:;.@+^/!%

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

Table 1-1 Configuration of CAA record sets

Function	Example CAA Record Set	Description
Configure a CAA record set for one domain name.	0 issue "ca.example.com "	Only the specified CA (**ca.example.com**) can issue certificates for a particular domain name (**domain.com**). Requests to issue certificates for the domain name by other CAs will be rejected.
	0 issue ";"	No CA is allowed to issue certificates for the domain name (**domain.com**).

Function	Example CAA Record Set	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/"	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 Planning

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

Table 1-2 Domain name

Service	Public Zone	Record Set Type
DNS	domain.com	CAA

Table 1-3 Resources and costs

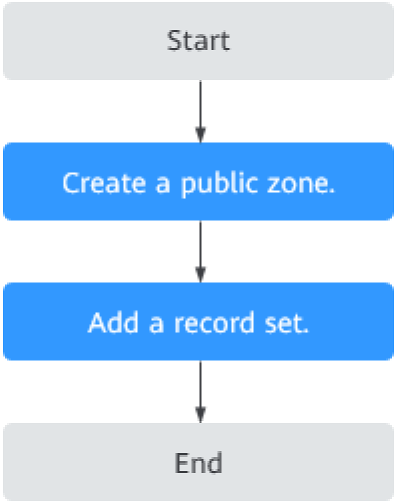
Service	Resource	Description	Quantity	Monthly Price
Domains	Domain name	Public domain name: domain.com	1	N/A

Service	Resource	Description	Quantity	Monthly Price
DNS	- Public zone - Record set	- Public zone: 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 1-2 shows the process for adding a CAA record set to a public zone.

Figure 1-2 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 1-4**.

Table 1-4 Parameters for creating a public zone

Parameter	Description	Example Value
Domain Name	Name of the public zone, which is the domain name you registered The domain name can include two levels in addition to the top-level domain. The following are two examples: – Subdomain of domain.com: abc.domain.com – Subdomain of domain.com.cn: abc.domain.com.cn 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 details about the email address, see **Why Was the Email Address Format Changed in the SOA Record?**	N/A
Tag	(Optional) Identifier of the domain name 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 1-5**. **NOTE** If you have configured tag policies for DNS, you need to add tags to your zones based on the tag policies. If you add a tag that does not comply with the tag policies, zones may fail to be created. Contact the administrator to learn more about tag policies.	example_key1 example_value1
Description	(Optional) Supplementary information about the zone The value cannot exceed 255 characters.	This is a zone example.

Table 1-5 Tag naming rules

Parameter	Requirements	Example Value
Tag 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 nor contain special characters =*<>\,|/	example_key1
Value	– Cannot be left blank. – Can contain a maximum of 43 characters. – Cannot start or end with a space nor contain special characters =*<>\,|/	example_value1

4. Click **OK**.

Step 2 Add a CAA record set.

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

   The record set page is displayed.
2. Click **Add Record Set**.

   The **Add Record Set** dialog box is displayed.
3. Configure the parameters based on **Table 1-6**.

Table 1-6 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 to be resolved is www.domain.com, which is used for a website. – Left blank: The domain name is domain.com. The **Name** field cannot be set to an at sign (@). Just leave this field 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.	Leave this parameter 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. 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 will return the IP address of the specific line, depending on where the visitors come from. This parameter is only designated for public domain names. – **Default**: returns the default resolution result irrespective of where the visitors come from. – **ISP**: returns the resolution result based on visitors' carrier networks. – **Region**: returns the resolution result based on visitors' 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 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 a maximum of 50 record values, 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, the value is set to **0**. – **tag**: You can enter 1 to 15 characters, consisting of letters and digits from 0 to 9. The tag can be one of the following: ▪ **issue**: authorizes a CA to issue all types of certificates. ▪ **issuewild**: authorizes a CA to issue wildcard certificates. ▪ **iodef**: requests notifications once a CA receives invalid certificate requests. – **value**: authorized CA or email address/URL required for notification once the CA receives invalid certificate requests. The value depends on the value of **tag** and must be enclosed in quotation marks (""). The value can contain a maximum of 255 characters, consisting of letters, digits, spaces, and special characters -#*?&_~=:;.@+^/!%	0 issue "ca.abc.com" 0 iodef "mailto:admin@domain.com"
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000**, and the default value is **1**. This parameter is only designated 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

Parameter	Description	Example Value
Tag	(Optional) Identifier of a record set. Each tag contains a key and a value. You can add a maximum of 10 tags to a record set. For details about tag key and value requirements, see **Table 1-7**. **NOTE** If you have configured tag policies for DNS, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.	example_key1 example_value1
Description	(Optional) Supplementary information about the record set. You can enter a maximum of 255 characters.	The description of the hostname.

Table 1-7 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 nor contain special characters =*<>\,|/	example_key1
Value	– Cannot be left blank. – Can contain a maximum of 43 characters. – Cannot start or end with a space nor contain special characters =*<>\,|/	example_value1

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

Copyright © Huawei Technologies Co., Ltd.

2 Configuring Private Domain Names for ECSs

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, you need to launch your website again.

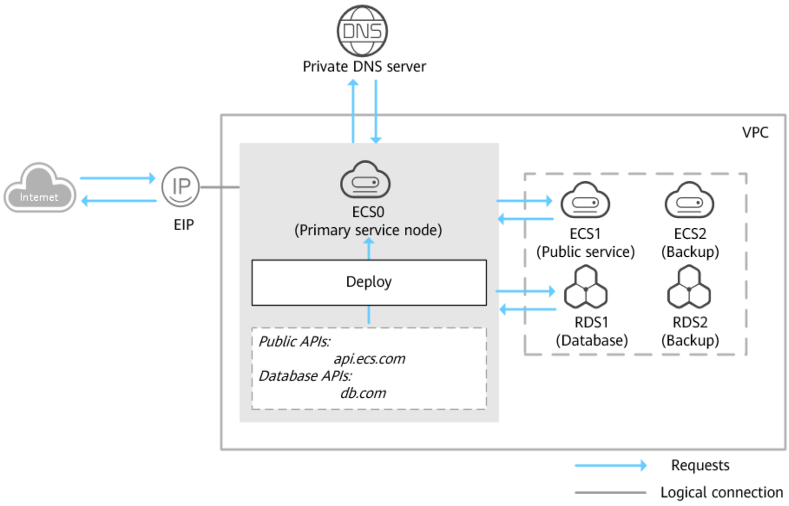
Here is the solution: Configure private domain names for the ECSs and include the private domain names in the code. If one ECS is malfunctioning, you only need to change the DNS record sets to direct traffic to a normal ECS. Your services will not be interrupted, and you do not need to launch the website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

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

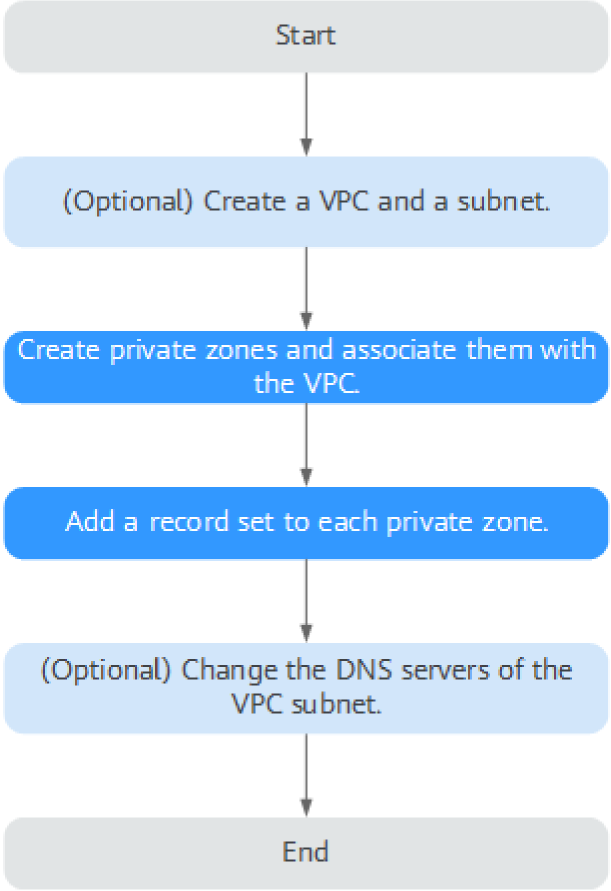
Table 2-2 Resource planning

Region	Service	Resource	Description	Quantity	Monthly Price
CN-Hong Kong	VPC	VPC_001	The DNS server addresses must be the same as the private DNS server addresses 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 server addresses of 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 as prompted. **Table 2-3** describes the key parameters.

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 server addresses of 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
VPC	VPC to be associated with the private zone	VPC_001

Parameter	Description	Example Value
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 details about the email address, see **Why Was 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 2-5**. **NOTE** If you have configured tag policies for DNS, you need to add tags to your zones based on the tag policies. If you add a tag that does not comply with the tag policies, zones may fail to be created. Contact the administrator to learn more about tag policies.	N/A
Description	(Optional) Description of a zone. The value cannot exceed 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 a maximum of 36 characters. – Cannot start or end with a space nor contain special characters =*<>\,|/	example_key1
Value	– Cannot be left blank. – Can contain a maximum of 43 characters. – Cannot start or end with a space nor contain special characters =*<>\,|/	example_value1

4. Click **OK**. Then check the private zone created for api.ecs.com.

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

   NOTE

   You can click the domain name to view SOA and NS record sets automatically generated for 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**. **NOTE** If you have configured tag policies for DNS, you need to add tags to your record sets based on the tag policies. If you add a tag that does not comply with the tag policies, record sets may fail to be created. Contact the administrator to learn more about tag policies.	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 **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, see **Table 2-2**.

Step 4 (Optional) Change the DNS server addresses 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 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 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**.

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

----End