Advanced Anti-DDoS

User Guide

Issue 26

Date 2020-11-09



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.

Contents

1 Enabling the AAD Service....1
1.1 Purchasing AAD Instances....1
1.2 Line Packages....5
1.3 Upgrading Specifications....8
2 Connecting a Website Service to AAD....11
3 Connecting a Non-website Service to AAD....21
4 Configuring a Forwarding Rule....27
5 Configuring a Protection Policy....32
5.1 Configuring a Blacklist and a Whitelist....32
5.2 Configuring Traffic Control....34
5.3 Configuring CC Attack Protection Rules....36
6 Adding a CNAME Record....43
7 Viewing Protection Details....48
8 Enabling Alarm Notification....52
9 Managing an Instance....55
9.1 Viewing Information About an Instance....55
9.2 Changing the Name of an AAD Instance....56
9.3 Changing the Elastic Protection Bandwidth....57
10 Managing a Forwarding Rule....59
10.1 Viewing Information About a Forwarding Rule....59
10.2 Changing an Origin Server IP Address....60
10.3 Deleting a Forwarding Rule....61
10.4 Exporting a Forwarding Rule....63
11 Managing a Domain Name....64
11.1 Viewing Information About a Domain Name....64
11.2 Enabling Basic Web Protection and CC Attack Protection....65
11.3 Updating a Certificate....66
11.4 Modifying Resolution Lines for High-Defense IP Addresses of a Domain Name....70
11.5 Modifying Domain Name Configuration....71

 Copyright © Huawei Technologies Co., Ltd.

11.6 Deleting a Domain Name 72
12 Viewing a Back-to-Origin IP Address Range 74
13 Viewing a Protection Report 76
14 (Optional) Managing Enterprise Projects 79
14.1 Creating an Enterprise Project 79
14.2 Disabling an Enterprise Project 80
14.3 Managing Enterprise Project Resources 81
14.4 Managing a User Group 83
14.5 Viewing Expenditures of an Enterprise Project 85
14.6 Unsubscribing from an Enterprise Project 86
15 Permissions Management 88
15.1 Creating a User and Granting the AAD Access Permission 88
A Change History 90

 Copyright © Huawei Technologies Co., Ltd.

1 Enabling the AAD Service

1.1 Purchasing AAD Instances

Scenarios

Before using Advanced Anti-DDoS (AAD), you must purchase AAD instances.

NOTE

Each user can purchase a maximum of five instances by default. If the quota is insufficient, **submit a service ticket** to apply for a higher quota.

Precautions

- Ensure that the account used for purchasing AAD instances has both the CAD Administrator and BSS Administrator roles or has the Tenant Administrator role.
  - **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
  - **Tenant Administrator**: has all permissions on all services except on IAM.
- After an AAD instance is purchased, the instance specifications cannot be modified.

Prerequisites

- AAD (Chinese Mainland) is recommended if your server is deployed in the Chinese Mainland. You have obtained an ICP license first before protecting your domain names.
- If your server is outside the Chinese Mainland, AAD (International) is recommended.

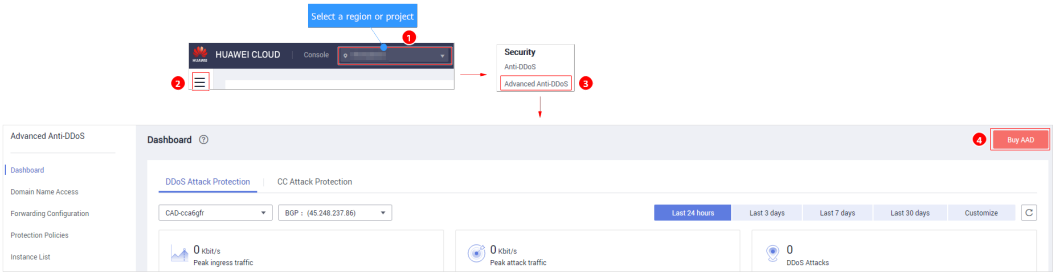
Procedure

Step 1 **Log in to the management console.**

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Figure 1-1 shows how to enter the AAD console page.

Figure 1-1 Entering the AAD console page



NOTE

Figure 1-1 describes how to enter the AAD console for customers who buy AAD for the first time. If you purchase AAD instance for the first time, perform the following steps:

1. Click ☰ in the upper left corner and choose **Security** > **Advanced Anti-DDoS**.
2. Click **Buy AAD**.

Step 3 On the displayed **Buy AAD** page, set required parameters shown in Figure 1-2. Table 1-1 describes the parameters to be configured.

Figure 1-2 Setting required parameters

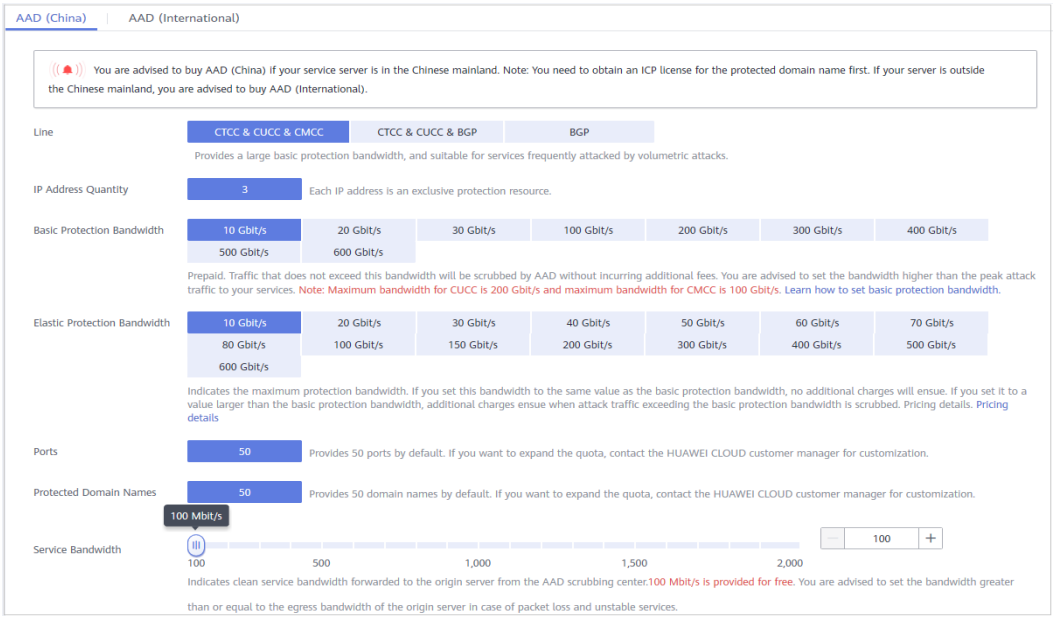


Table 1-1 Parameter description

Parameter	Description	Example Value
Line	Lines **CTCC & CUCC & CMCC**, **CTCC & CUCC & BGP**, and **BGP** are supported.	**CTCC & CUCC & CMCC**:

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
IP Address Quantity	Specifies the number of high-defense IP addresses automatically assigned to the line. The high-defense IP address is provided exclusively for each of your service system. **NOTE** The IP addresses are the ones assigned by AAD and used for providing services for customers in place of the origin server IP address.	3
Basic Protection Bandwidth	Value range: • **CTCC & CUCC & CMCC**: **10 Gbit/s** to **600 Gbit/s** • **CTCC & CUCC & BGP**: **10 Gbit/s** to **30 Gbit/s** • **BGP**: **10 Gbit/s** and **20 Gbit/s** Traffic that does not exceed this bandwidth will be scrubbed by AAD without incurring additional fees. To achieve enhanced protection, use the **Elastic Protection Bandwidth** parameter.	10 Gbit/s
Elastic Protection Bandwidth	Value range: • **CTCC & CUCC & CMCC**: **10 Gbit/s** to **600 Gbit/s** • **CTCC & CUCC & BGP**: **10 Gbit/s** to **600 Gbit/s** • **BGP**: **10 Gbit/s** to **200 Gbit/s** If you set this parameter to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is scrubbed. If the attack traffic exceeds the elastic protection bandwidth, the high-defense IP address will be blocked by a black hole and cannot provide services. You can modify the elastic protection bandwidth as needed after you have purchased an AAD instance. **NOTE** • The elastic protection bandwidth must be greater than or equal to the basic protection bandwidth. If the two are set to the same value, the elastic protection bandwidth function does not take effect. • **Line Packages** describes the elastic protection bandwidth ranges in different scenarios.	10 Gbit/s

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Ports	Specifies the number of ports an AAD instance can protect. 50 ports can be protected for free by default. You can **submit a service ticket** to apply for a quota increase.	50
Protected Domain Names	Specifies the number of domain names an AAD instance can protect. 50 domain names can be protected for free by default. You can **submit a service ticket** to apply for a quota increase.	50
Service Bandwidth	Specifies the service bandwidth for the AAD instance to forward scrubbed traffic to origin servers. The value ranges from **100 Mbit/s** to **2000 Mbit/s**.	100

Step 4 Set **Required Duration** and **Quantity**, as shown in **Figure 1-3**. **Table 1-2** describes the parameters.

Figure 1-3 Setting **Required Duration** and **Quantity**

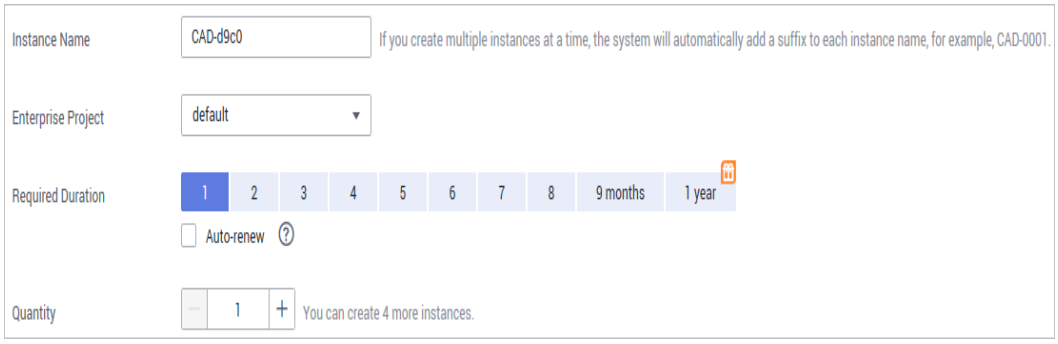


Table 1-2 Parameter description

Parameter	Description	Example Value
Instance Name	Enter a name for the AAD instance you are purchasing. • The name can contain a maximum of 32 characters. • The name can contain only letters, digits, underscores (_), and hyphens (-).	CAD-0001
Enterprise Project	This parameter can only be set by enterprise project users.	N/A
Required Duration	Select a value from one month to one year.	1

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Quantity	Select the number of instances to be purchased. By default, each user can purchase a maximum of five instances.	1

NOTE

The **Auto-renew** option is optional. If you tick **Auto-renew**, the system will automatically renew the AAD instance before it expires.

Step 5 Click **Next**.

Step 6 On the **Confirm** page, confirm your order and click **Submit Order**.

Step 7 On the **Pay** page, click **Pay** to pay for the order.

Step 8 When **Order submitted successfully** is displayed, choose **Service List** > **Security** > **Advanced Anti-DDoS**. The instance list is displayed.

----End

1.2 Line Packages

Currently, AAD offers three line packages:

- CTCC & CUCC & CMCC
- CTCC & CUCC & BGP
- BGP

NOTE

These line packages apply only to AAD instances that will protect your servers deployed in the Chinese Mainland. If your servers are deployed outside the Chinese Mainland, visit the international website.

NOTICE

Ensure that the account used for purchasing lines has both the CAD Administrator and BSS Administrator roles or has the Tenant Administrator role.

- **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
- **Tenant Administrator**: has all permissions on all services except on IAM.

Copyright © Huawei Technologies Co., Ltd.

Line Specifications and Application Scenarios

Line	Basic Protection Bandwidth	Elastic Protection Bandwidth	Application Scenario
CTCC & CUCC & CMCC:	10 Gbit/s to 600 Gbit/s	A maximum of 600 Gbit/s for CTCC, 600 Gbit/s for CUCC, and 100 Gbit/s for CMCC	This line package applies to service systems that have a large user group and have connections to the networks of all three carriers. It protects services against volumetric flooding attacks.
CTCC & CUCC & BGP:	10 Gbit/s to 30 Gbit/s	A maximum of 600 Gbit/s for CTCC, 200 Gbit/s for CUCC, and 200 Gbit/s for BGP (The maximum bandwidth for BGP is dynamically adjusted based on the real-time network traffic, sometimes lower than 200 Gbit/s.)	This line package applies to service systems that have a large user group and have connections to the networks of the three carriers, China Education and Research Network (CERNET), and China Mobile Tietong. It comprises both better user experience of the BGP line and protection against volumetric flooding attacks.
BGP	10 Gbit/s to 20 Gbit/s	A maximum of 200 Gbit/s (The maximum bandwidth is dynamically adjusted based on the real-time network traffic, sometimes lower than 200 Gbit/s.)	This line package addresses the requirements for accessing the networks of CTCC, CUCC and other carriers (such as CMCC, CERNET, China Mobile Tietong, and Great Wall Broadband Network) and for defending against flooding attacks smaller than 200 Gbit/s. The maximum basic protection bandwidth is 20 Gbit/s, and the maximum elastic protection bandwidth is 200 Gbit/s.

Copyright © Huawei Technologies Co., Ltd.

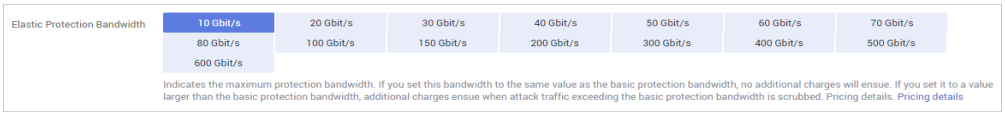
Elastic Protection Bandwidth

The elastic protection bandwidth is set to a value greater than or equal to the basic protection bandwidth.

If you set this bandwidth to the same value as the basic protection bandwidth, no additional charges will ensue. If you set it to a value larger than the basic protection bandwidth, the maximum protection capability is determined by the elastic protection bandwidth you set. Additional charges ensue when attack traffic exceeding the basic protection bandwidth is scrubbed. For details about the charging, see **Product Pricing Details**.

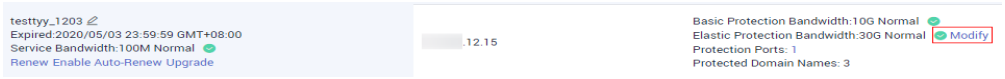
- You can set the elastic protection bandwidth when you purchase the AAD instance on the **Buy AAD** page.

  Figure 1-4 Setting **Elastic Protection Bandwidth**

- You can click **Modify** to adjust the elastic protection bandwidth based on the actual requirements on the console, as shown in **Figure 1-5**. If you set this bandwidth to the same value as the basic protection bandwidth, no additional charges will ensue. If you set it to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is scrubbed. For details about the pricing details, see **Product Pricing Details**.

  Figure 1-5 Modifying the elastic protection bandwidth

CTCC & CUCC & CMCC:

You will obtain three high-defense IP addresses respectively for the CTCC, CUCC, and CMCC lines. CTCC offers a maximum of 600 Gbit/s elastic protection, CUCC 600 Gbit/s, and CMCC 100 Gbit/s.

NOTICE

- You need to obtain an ICP license first before protecting your website domain names using the CTCC, CUCC, and CMCC lines.
- If a user visits the website over the network of another carrier other than CTCC, CUCC, and CMCC, packet loss or delay may occur due to cross-network data transmission. To avoid this problem, you are advised to use the BGP line.

CTCC & CUCC & BGP:

You will obtain three high-defense IP addresses respectively for the CTCC, CUCC, and BGP lines. Each line has a basic protection bandwidth of 20 Gbit/s. The two high-defense IP addresses of CTCC and CUCC have a maximum elastic protection

 Copyright © Huawei Technologies Co., Ltd.

capability of 600 Gbit/s and 200 Gbit/s respectively. The BGP line also supports elastic protection. Its maximum elastic protection bandwidth is dynamically adjusted from 20 Gbit/s to 200 Gbit/s depending on real-time network traffic.

The BGP line is able to connect networks of different carriers smoothly, preventing the cross-network transmission problems.

You are advised to configure the same forwarding rules for the three IP addresses to achieve optimal protection capability and access experience.

NOTICE

You need to obtain an ICP license first before protecting your website domain names using the CTCC, CUCC, and BGP lines.

BGP

You will obtain a high-defense IP address for the BGP line. You can set the basic protection bandwidth for 10 Gbit/s or 20 Gbit/s. This line is recommended for defending against attacks less than 200 Gbit/s. If the DDoS attack traffic exceeds the basic protection bandwidth, the high-defense IP address will be blocked by a black hole.

NOTICE

You need to obtain an ICP license first before protecting your website domain names using the BGP line.

1.3 Upgrading Specifications

Scenarios

This topic describes how to modify the basic protection bandwidth, elastic protection bandwidth, and service bandwidth for an AAD instance.

NOTE

- The basic protection bandwidth and service bandwidth can be increased only.
- The lines cannot be changed during the upgrade.
- Expired instances do not support specifications upgrades.
- Frozen instances do not support specifications upgrades.

Prerequisites

You have obtained an account and its password to log in to the management console.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

Ensure that the account used for upgrading the specifications of AAD instances has both the CAD Administrator and BSS Administrator roles or has the Tenant Administrator role.

- **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
- **Tenant Administrator**: has all permissions on all services except on IAM.

Fees Description

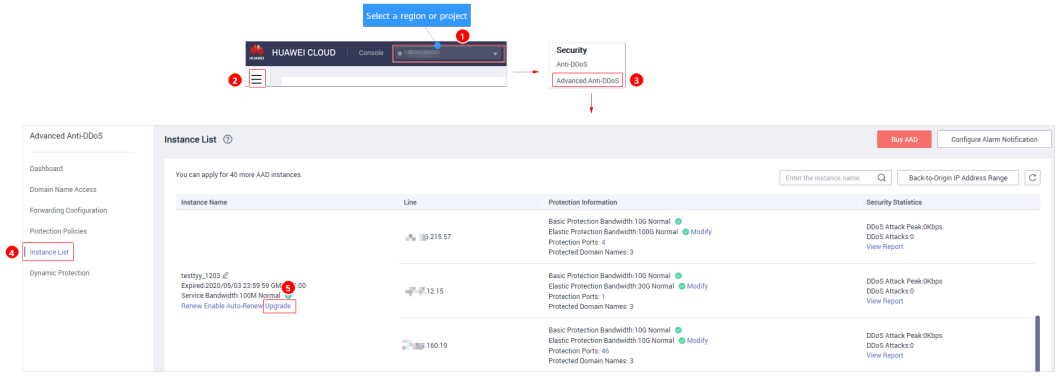
Modifying specifications will lead to fee changes. For details, see **Pricing of a Changed Specification**.

Procedure

Step 1 **Log in to the management console.**

Step 2 Log in to the management console. Follow the procedure shown in the following figure to locate the target instance and click **Upgrade**.

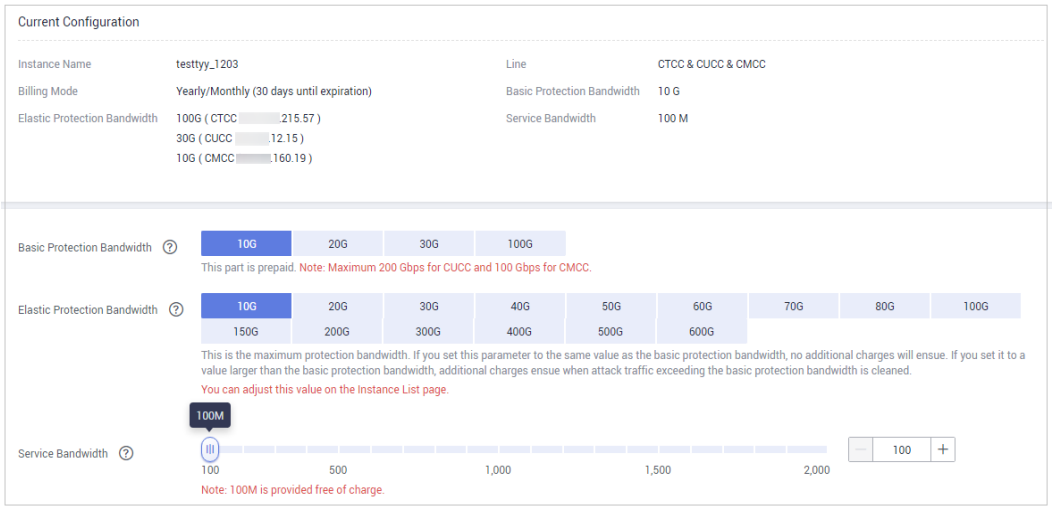
Figure 1-6 Specifications upgrading entry



Step 3 On the displayed page, configure **Basic Protection Bandwidth**, **Elastic Protection Bandwidth**, and **Service Bandwidth**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-7 Upgrading specifications



Step 4 After you click **Submit**, the system will determine whether the configuration has changed. If the configuration does not change, the system displays a failure message indicating that selected specifications are the same as original specifications. If the configuration has changed, the **Details** page is displayed.

Step 5 Click **Submit Order**. When the payment is successful, the **Order submitted successfully** page is displayed.

----End

 Copyright © Huawei Technologies Co., Ltd.

2 Connecting a Website Service to AAD

Scenarios

You can use the Canonical Name (CNAME)-based access to connect your website service to AAD so that access traffic will be directed to the high-defense IP address. A CNAME record is a type of DNS record that maps an alias name to a true or canonical domain name.

Each AAD instance can protect a maximum of 50 domain names. Domain names that need to be protected cannot be added in batches.

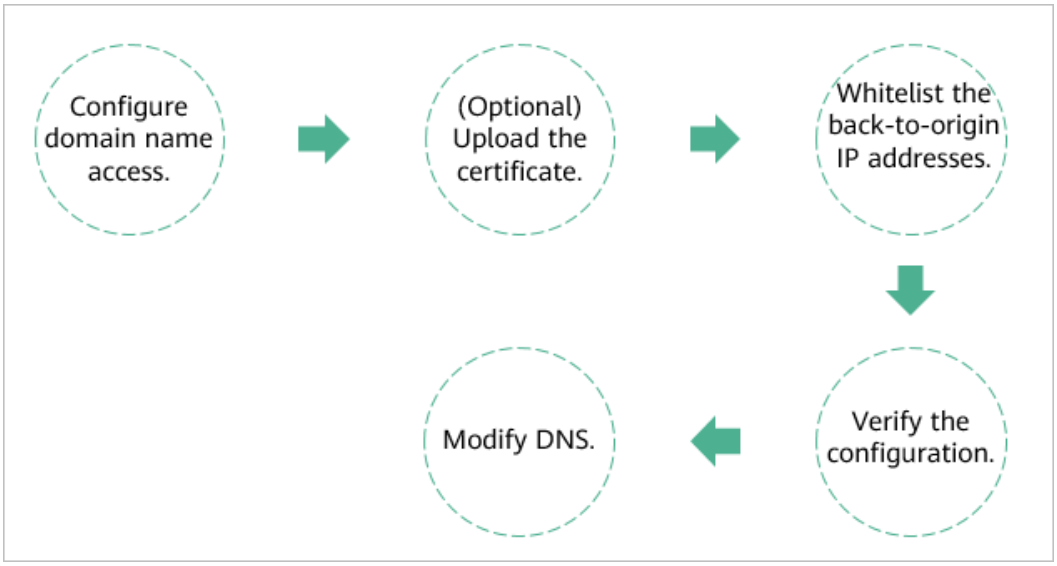
Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

Procedure

Figure 2-1 shows the procedure for accessing website services.

Figure 2-1 Procedure for accessing website services

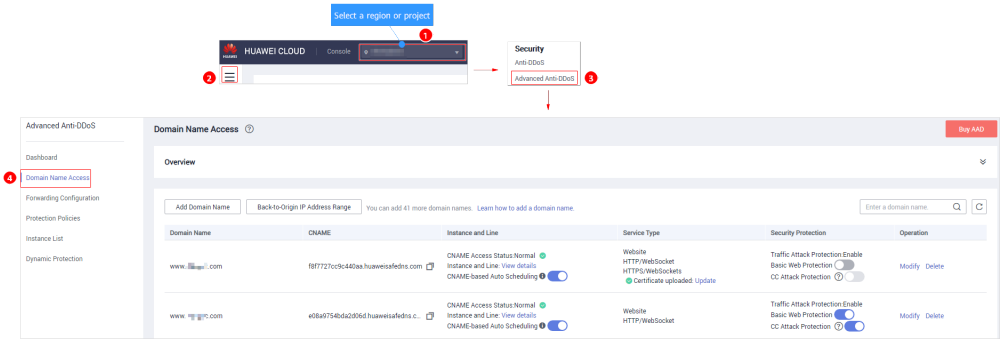


 Copyright © Huawei Technologies Co., Ltd.

Step 1 **Log in to the management console.**

Step 2 Follow the procedure shown in the following figure to enter the **Domain Name Access** page.

Figure 2-2 Domain Name Access page

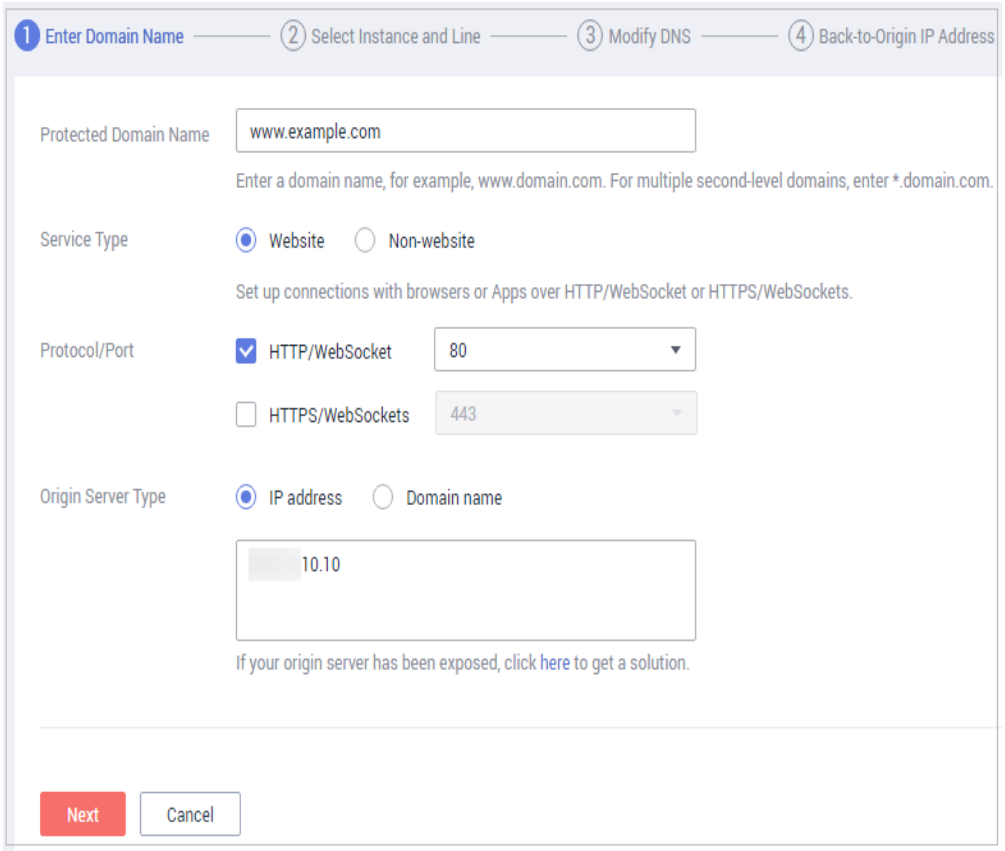


Step 3 On the displayed page, click **Add Domain Name**.

Step 4 Configure domain name access.

1. Set required parameters on the displayed page. **Table 2-1** describes the parameters. Click **Next** after the parameters are all configured.

Figure 2-3 Entering domain name information for a website service



 Copyright © Huawei Technologies Co., Ltd.

NOTE

If you log in to the management console using an enterprise project account, you can choose **Enterprise** > **Project Management** in the upper right corner. On the displayed page, choose **Project Management** in the navigation pane on the left, and select the target project.

Table 2-1 Parameter description

Parameter	Description	Example Value
Protected Domain Name	Enter the domain name of the service to protect. – Single domain name: Enter a single domain name, for example, www.example.com. – Wildcard domain name ▪ If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can directly add the wildcard domain name ****.example.com*** to AAD for protection. ▪ If the server IP addresses of subdomain names are different, add subdomain names one by one.	Single domain name: **www.example.com** Wildcard domain name: ***.example.com**
Service Type	Select **Website**.	Website
Protocol/ Port	Select a port based on your needs. – Available HTTP/WebSocket ports are **80**, **81**, **82**, **83**, **84**, **8006**, **8078**, **8080**, **8081**, **8087**, **8097**, **19101**, **19501**, **21028**, **40009**, and **40010**. – Available HTTPS/WebSocket ports are **443**, **4006**, **4443**, **5443**, **6443**, **7443**, **8443**, **9443**, **14443**, **20000**, **28443**, **30001**, **30002**, **30003**, **30004**, and **30005**. **NOTE** In one line, website services and non-network services cannot use the same port number.	80

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Origin Server Type	Origin server type of the protected domain name to be added. The value of this parameter can be: – IP address IP address of a real server. A maximum of 20 IP addresses can be entered. Use commas (,) to separate the IP addresses. – Domain name Currently, only HUAWEI CLOUD WAF CNAME is supported. **NOTICE** – If the protected domain name to be added shares the high-defense IP address and protocol or port with a domain name, the values of **Origin Server Type** for the domain names must be same. ▪ If **Origin Server Type** is set to **IP address** for a domain name, ensure the web protection is enabled for the domain name. For details about how to enable the web protection, see **Step 4.7**. ▪ If **Origin Server Type** is set to **Domain name** for a domain name, ensure that the domain name and the protected domain name to be added are connected to the same WAF. – If **Origin Server Type** is set to **Domain name**, ensure that the domain name has been allowed to use a proxy. Otherwise, the service may be unavailable after being connected to AAD. – If you connect your service to AAD using a WAF CNAME but no longer need WAF protection, delete the service domain name from AAD first.	IP address

2. (Optional) Upload a certificate.

   If you have selected **HTTPS/WebSockets** and set **Origin Server Type** to **IP address**, perform the following steps to upload or update a certificate:

   You can select an existing certificate from the drop-down list or upload a certificate. To upload a certificate, perform the following steps:

   a. Click **Upload Certificate**.

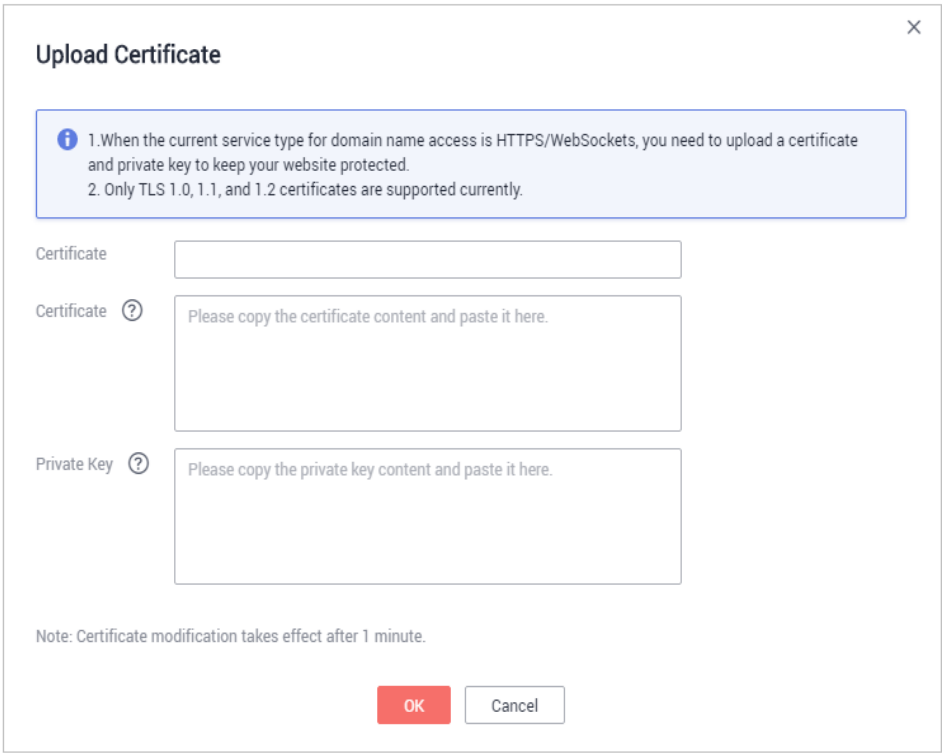
   b. In the displayed **Upload Certificate** dialog box, enter the domain name, certificate content, and private key. **Table 2-2** describes the required parameters.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

The certificate name contains a maximum of 10 characters and cannot contain special characters.

Figure 2-4 Uploading a certificate



NOTE

- Currently, only TLS 1.0, TLS 1.1, and TLS 1.2 certificates can be uploaded.
- You can select an existing certificate.
- Each certificate name of a user must be unique.
- You can select an existing certificate through fuzzy search.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-2 Parameter description

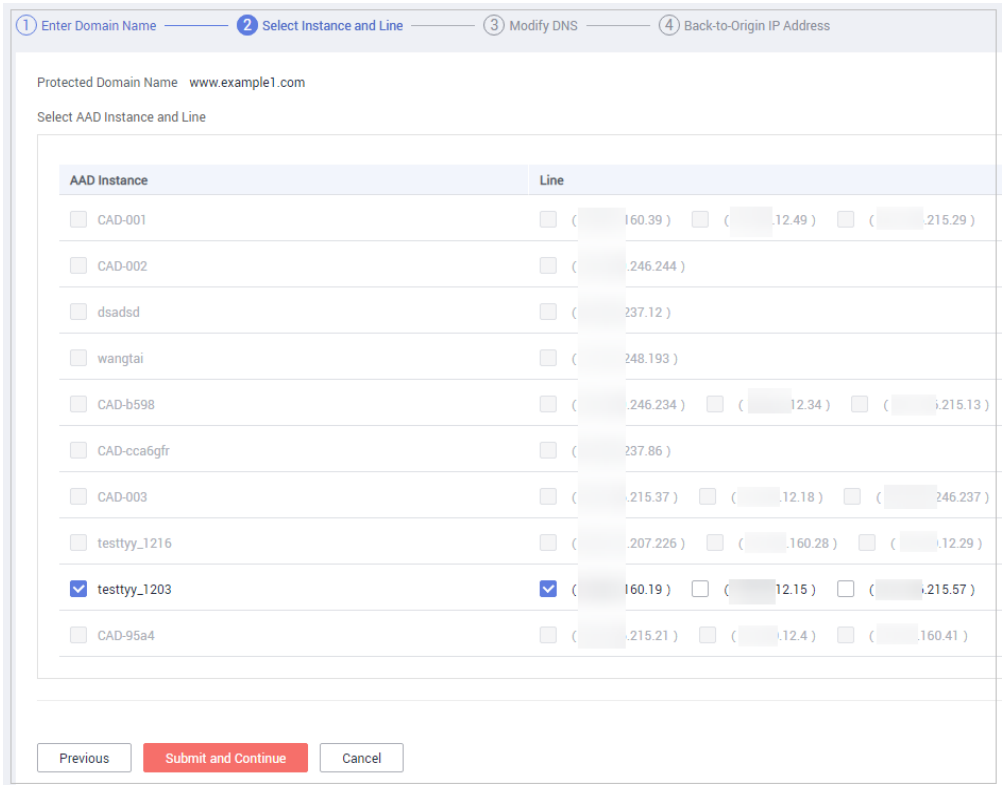
Parameter	Description
Certificate	■ The certificate must be in the following format: -----BEGIN CERTIFICATE----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYD VQQGEwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3 ZWkxDzANBgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZz ZXJ2ZXIxIjAgBgkqhkiG9w0BCQEWE3p3YW5nd2VpZGtkQDE2My5jb20wHhcNMTUw MzE4MDMzNjU5WhcNMjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNV BAgTAlpKMQswCQYDVQQHEwJIWjEPMA0GA1UEChMGaHVhda2VpMQ8wDQY..... -----END CERTIFICATE----- ■ Method for you to copy your certificate: ○ For a .pem certificate: Use a text editor to open the certificate file and copy the content here. ○ For other certificates: Convert your certificate to a .pem one. Then open it with a text editor and copy its content. **NOTE** For details about how to convert a certificate, see **How Do I Convert a Non-PEM Certificate into a PEM One?**.
Private Key	The private key must be in the following format: -----BEGIN RSA PRIVATE KEY----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYDVQQG EwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3ZWkxDzAN BgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZzZXJ2ZXIxIjAg BgkqhkiG9w0BCQEWE3poYW5nd2VpZGtkQDE2My5jb20wHhcNMTUwMzE4MDMzNjU5WhcN MjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAlpKMQswCQYDVQQH EwJIWjEPMA0GA1UEChMGaHVhd2VpMQ8wDQYDVQQLEwZ -----END RSA PRIVATE KEY----- ■ Method for you to copy your private key: ○ For a .pem file: Use a text editor to open the private key file and copy the content here. ○ For other certificates: Convert your certificate to a .pem one. Then open it with a text editor and copy its content. **NOTE** For details about how to convert a certificate, see **How Do I Convert a Non-PEM Certificate into a PEM One?**.

c. Click **OK**.

3. Select required AAD instances and lines and click **Submit and Continue**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-5 Select Instance and Line

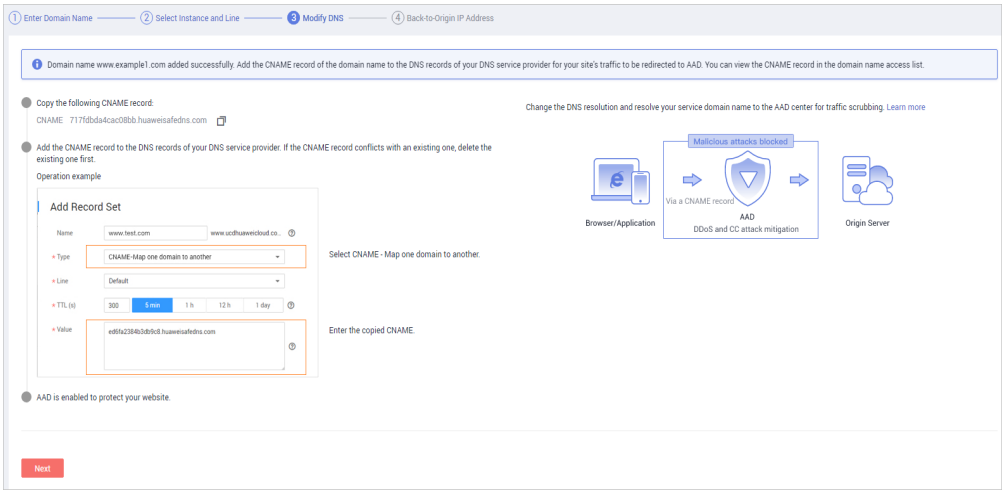


NOTE

- You can select multiple lines (with high-defense IP addresses) for a domain name. However, the IP addresses must have the same number of forwarding rules, the same forwarding protocols, ports, and the same service type.
- HUAWEI CLOUD provides multiple carrier lines for each instance to avoid cross-carrier access from your users. You are advised to select a complete set of lines, which includes all carriers, when selecting lines for your instance.

4. Copy the displayed CNAME record of the domain name and add the CNAME to DNS. Then click **Next**.

Figure 2-6 Modifying DNS

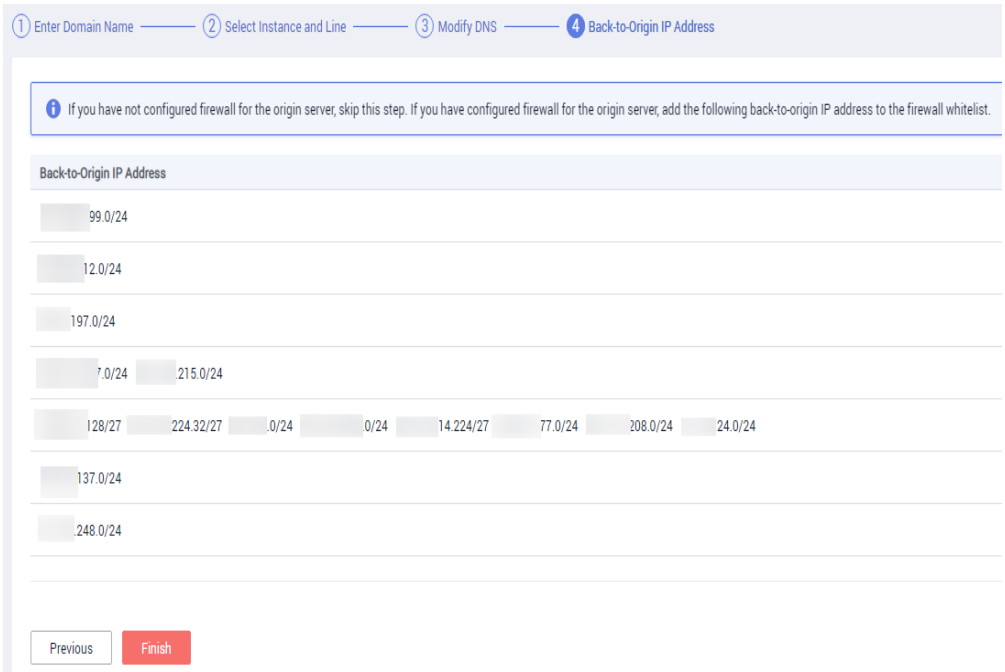


 Copyright © Huawei Technologies Co., Ltd.

For details about modifying DNS configuration, see **Adding a CNAME Record**.

5. Add the back-to-origin IP addresses to the firewall whitelist.

Figure 2-7 Adding the back-to-origin IP addresses to the firewall whitelist



- If no firewall has been configured for the origin server, click **Finish**.
- If a firewall has been configured for the origin server, whitelist the back-to-origin IP addresses on the firewall, ACL, or any other security software of your origin servers to prevent the access traffic from being blocked or limited by the security policies. Click **Finish**.

The **Domain Name Access** page is displayed. The newly added domain name is displayed in the list.

NOTE

AAD executes Full Network Address Translation (Full-NAT) and diverts access traffic to the back-to-origin IP addresses.

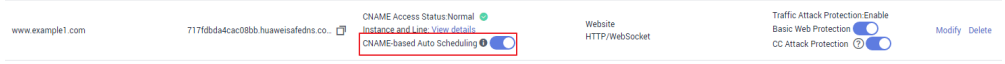
- If AAD is not used, access traffic is sent directly from the source IP addresses of clients towards origin servers. From the view of origin servers, the requests originate from scattered clients and each source IP address sends only a few access requests.
- After AAD is enabled, access traffic will be forwarded to the back-to-origin IP addresses. From the view of origin servers, the requests originate from these back-to-origin IP addresses. These IP addresses are fixed and limited in quantity, and each carries more requests than the source IP address. Therefore, they may be mistakenly regarded as the sources that launch attacks. In this case, other Anti-DDoS security policies working on the origin servers may block or limit the requests from the back-to-origin IP addresses. For example, error 502 is reported if the access request is blocked by mistake.

6. (Optional) Enable CNAME-based auto scheduling.

   CNAME-based auto schedule distributes incoming traffic based on its originating carrier. It can divert traffic to other lines if a line is blocked by a black hole.

 Copyright © Huawei Technologies Co., Ltd.

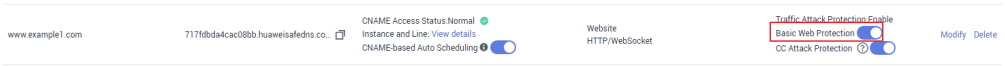
Figure 2-8 Enabling CNAME-based automatic scheduling



7. (Optional) If you set **Origin Server Type** to **IP address**, locate the row containing the target domain name and enable **Basic Web Protection** in the **Security Protection** column, as shown in **Figure 2-9**.

   AAD provides you with layer-7 protection only after you enable basic web protection.

Figure 2-9 Enabling basic web protection



Step 5 Verify the configuration.

After the configuration takes effect, AAD is expected to forward the packets sent to the high-defense IP address or AAD CNAME to the origin servers. To ensure service stability, you can use the following steps to verify the configuration:

- **Assumed CNAME:**
  - CNAME: 5dc728e1769ad666.huaweisafedns.com
- **Procedure:**
  a. Use **Telnet www.huaweicloud.com 80** to verify the network connectivity.
     - If the connection setup is successful, you can Telnet to the public IP address from your local network environment.
     - If the connection setup fails, change your test network environment and try again. Some enterprises may have internal network constraints and fail the verification. For example, you can connect to the personal hotspot of your phone to verify the connectivity.

  b. After verifying the network connectivity, you can Telnet to the AAD CNAME over port 80.
     - If the Telnet command is executed successfully, the configuration has taken effect.
     - If the command execution fails, check whether the required steps have been completed.
     - If the fault persists, contact technical support.

Step 6 Modify DNS.

For details, see **Adding a CNAME Record**.

The DNS configuration takes effect after a period of time. In this period, you can test the domain name resolution using some online test tools such as 17ce and China Webmaster.

----End

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

- If you do not want a domain name to be resolved to a high-defense IP address, locate the row containing the domain name on the **Domain Name Access** page and click **View details** in the **Instance and Line** column. On the page that is displayed, click  for the target high-defense IP address to set **DNS Resolution** to .
- If you do not want to protect a domain name, locate the row containing the domain name on the **Domain Name Access** page and click **Delete** in the **Operation** column.

Copyright © Huawei Technologies Co., Ltd.

3 Connecting a Non-website Service to AAD

Scenarios

Non-website services include Apps and PC client services. For such services, you can configure CNAME records in DNS or directly configure high-defense IP addresses on clients to use AAD.

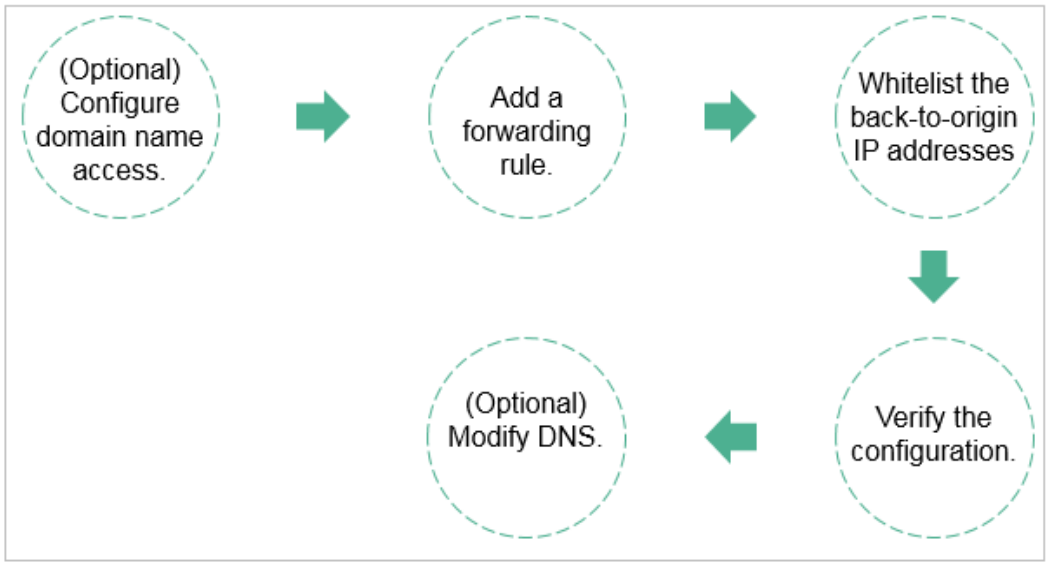
Prerequisites

- You have obtained an account and its password to log in to the management console.
- You have purchased an AAD instance.

Procedure

Figure 3-1 shows the procedure for accessing non-website services.

Figure 3-1 Procedure for accessing non-website services



 Copyright © Huawei Technologies Co., Ltd.

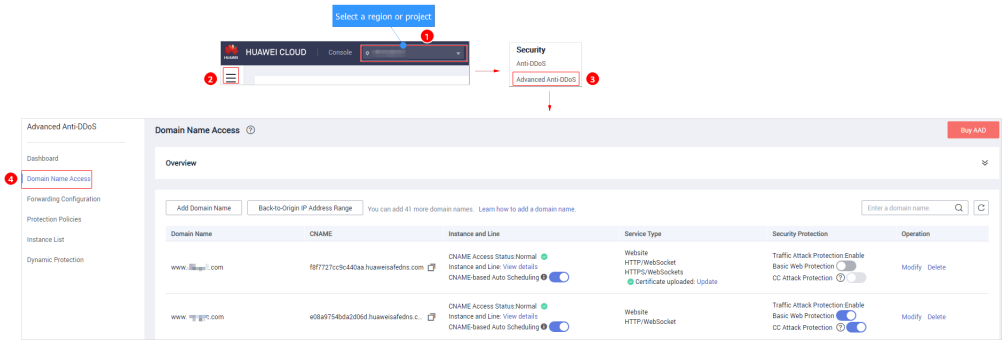
Step 1 **Log in to the management console.**

Step 2 (Optional) Configure domain name access.

Perform this step if intelligent resolution lines will be provided for domain names.

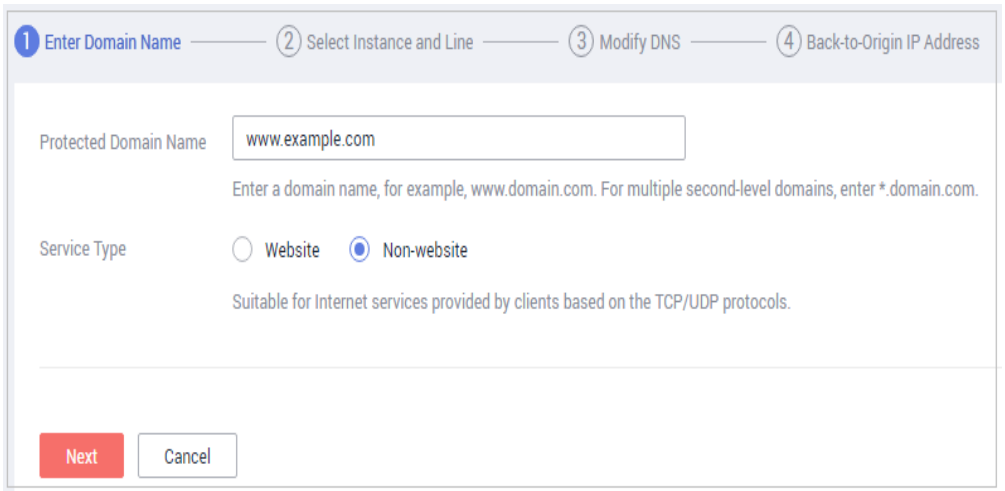
1. **Log in to the management console.**
2. Follow the procedure in the following figure to enter the **Domain Name Access** page.

Figure 3-2 Domain Name Access page



3. On the displayed page, click **Add Domain Name**.
4. Complete the necessary domain name information and click **Next**.

Figure 3-3 Entering domain name information for a non-website service



NOTE

If you log in to the management console using an enterprise project account, you can choose **Enterprise** > **Project Management** in the upper right corner. On the displayed page, choose **Project Management** in the navigation pane on the left, and select the target project.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-1 Parameter description

Parameter	Description
Protected Domain Name	Enter the domain name of the service to protect. – Single domain name: Enter a single domain name, for example, www.example.com. – Wildcard domain name ▪ If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can directly add the wildcard domain name ****.example.com*** to AAD for protection. ▪ If the server IP addresses of subdomain names are different, add subdomain names one by one.
Service Type	Select **Non-website**.

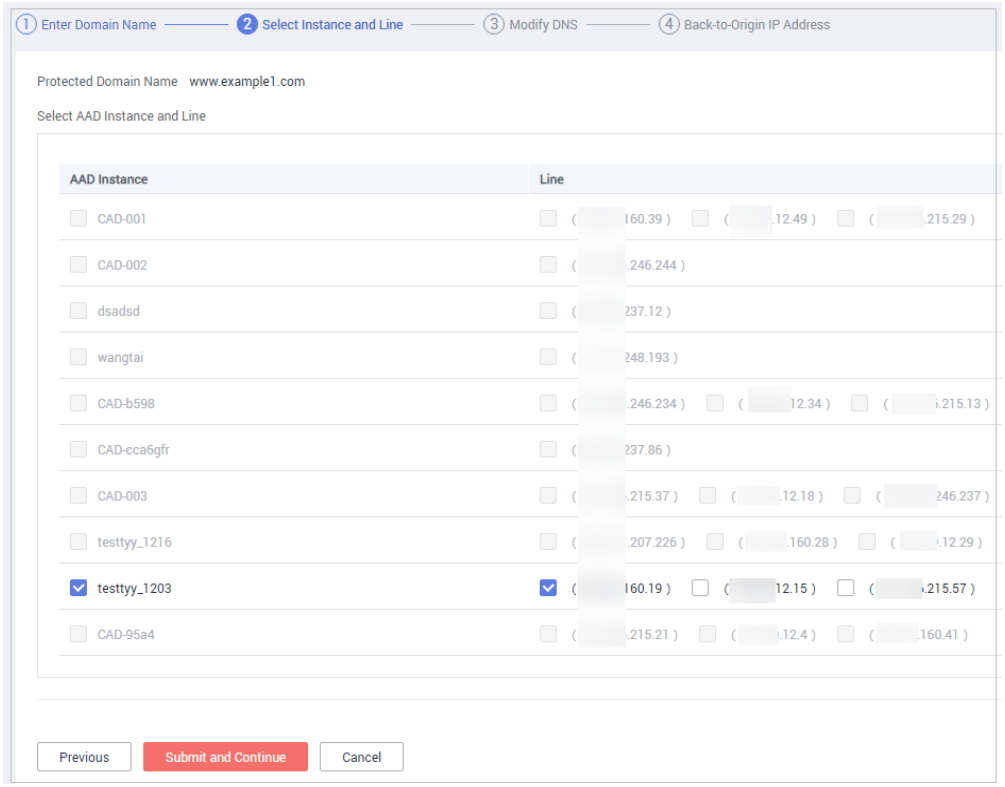
5. Select required AAD instances and lines and click **Submit and Continue**.

   You can select multiple lines (with high-defense IP addresses) for a domain name. However, the IP addresses must have the same number of forwarding rules, the same forwarding protocols, ports, and the same service type.

   HUAWEI CLOUD provides multiple carrier lines for each instance to avoid cross-carrier access from your users. You are advised to select a complete set of lines, which includes all carriers, when selecting lines for your instance.

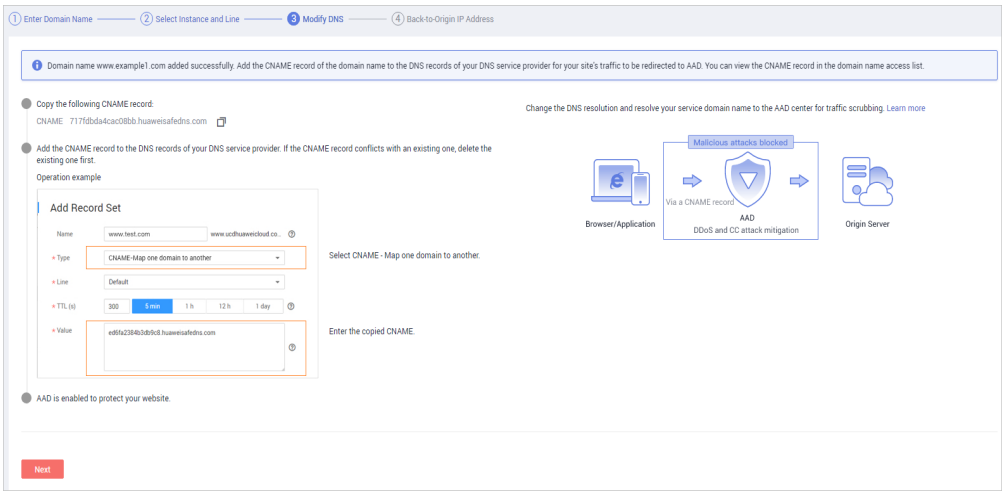
 Copyright © Huawei Technologies Co., Ltd.

Figure 3-4 Select Instance and Line



6. Copy the displayed CNAME record of the domain name and click **Next**.

Figure 3-5 Modifying DNS



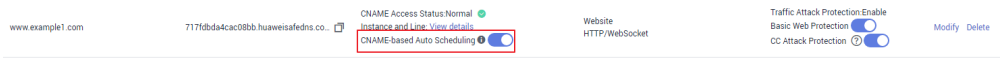
7. Whitelist the back-to-origin IP addresses.
   - If no firewall has been configured for the origin server, click **Finish**.
   - If a firewall has been configured for the origin server, add the back-to-origin IP address range to the whitelist of the firewall. Then click **Finish**.

   The **Domain Name Access** page is displayed. The newly added domain name is displayed in the list.
8. (Optional) Enable CNAME-based auto scheduling if you need to access the service using a domain name. CNAME-based auto schedule distributes

 Copyright © Huawei Technologies Co., Ltd.

incoming traffic based on its originating carrier. It can divert traffic to other lines if a line is blocked by a black hole.

Figure 3-6 Enabling CNAME-based automatic scheduling



Step 3 Add a forwarding rule.

For details, see **Configuring a Forwarding Rule**.

Step 4 Whitelist the back-to-origin IP addresses.

- Reason for whitelisting the IP addresses:

  AAD executes Full Network Address Translation (Full-NAT) and diverts access traffic to the back-to-origin IP addresses.

  - If AAD is not used, access traffic is sent directly from the source IP addresses of clients towards origin servers. From the view of origin servers, the requests originate from scattered clients and each source IP address sends only a few access requests.
  - After AAD is enabled, access traffic will be forwarded to the back-to-origin IP addresses. From the view of origin servers, the requests originate from these back-to-origin IP addresses. These IP addresses are fixed and limited in quantity, and each carries more requests than the source IP address. Therefore, they may be mistakenly regarded as the sources that launch attacks. In this case, other anti-DDoS security policies working on the origin servers may block or limit the requests from the back-to-origin IP addresses. For example, error 502 is reported if the access request is blocked by mistake.

- Procedure:

  a. View the back-to-origin IP address range. For details, see **Viewing a Back-to-Origin IP Address Range**.

  b. Whitelist the back-to-origin IP address range on the firewall, ACL, or any other security software on your origin servers to prevent the access traffic from being blocked or limited by the security policies.

Step 5 Verify the configuration.

After the configuration takes effect, AAD is expected to forward the packets sent to the high-defense IP address or AAD CNAME to the origin servers. To ensure service stability, you can use the following steps to verify the configuration:

- **Assumed parameter values:**
  - Lines: CTCC, CUCC, and CMCC
    - CTCC IP address: 1.1.1.1
    - CUCC IP address: 2.2.2.2
    - CMCC IP address: 3.3.3.3
  - CNAME: 5dc728e1769ad666.huaweisafedns.com
  - Forwarding port: 1234

 Copyright © Huawei Technologies Co., Ltd.

  - Protected domain name: www.test.com
  - Origin server IP address: 4.4.4.4
  - Origin server port: 1234
- **Procedure:**

  a. Use **Telnet www.huaweicloud.com 80** to verify the network connectivity.

     - If the connection setup is successful, you can Telnet to the public IP address from your local network environment.
     - If the connection setup fails, change your test network environment and try again. Some enterprises may have internal network constraints and fail the verification. For example, you can connect to the personal hotspot of your phone to verify the connectivity.

  b. After verifying the network connectivity, you can Telnet to the high-defense IP address of each carrier line and the AAD CNAME over port 1234.

     - If the Telnet command is executed successfully, the configuration has taken effect.
     - If the command execution fails, check whether the required steps have been completed.
     - If the fault persists, contact HUAWEI CLOUD technical support.

Step 6 (Optional) Modify DNS.

Perform this step if you need to access the service using a domain name.

- If you have configured domain name access and obtained the CNAME, perform **Adding a CNAME Record**.
- If you added a forwarding rule without configuring domain name access, perform **Adding an A Record**.

The DNS configuration takes effect after a period of time. In this period, you can test the domain name resolution using some online test tools such as 17ce and China Webmaster.

----End

Follow-up Procedure

- If you do not want a domain name to be resolved to a high-defense IP address, locate the row containing the domain name on the **Domain Name Access** page and click **View details** in the **Instance and Line** column. On the page that is displayed, click  for the target high-defense IP address to set **DNS Resolution** to .
- If you do not want to protect a domain name, locate the row containing the domain name on the **Domain Name Access** page and click **Delete** in the **Operation** column.

 Copyright © Huawei Technologies Co., Ltd.

4 Configuring a Forwarding Rule

Scenarios

If your instance runs a non-website service, you need to configure forwarding rules for the instance.

By default, you can add a maximum of 50 forwarding rules to each instance. you can **submit a service ticket** to add more forwarding rules.

After configuring the rules, change the domain names based on your services. AAD will automatically forward traffic to your origin server IP addresses.

Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

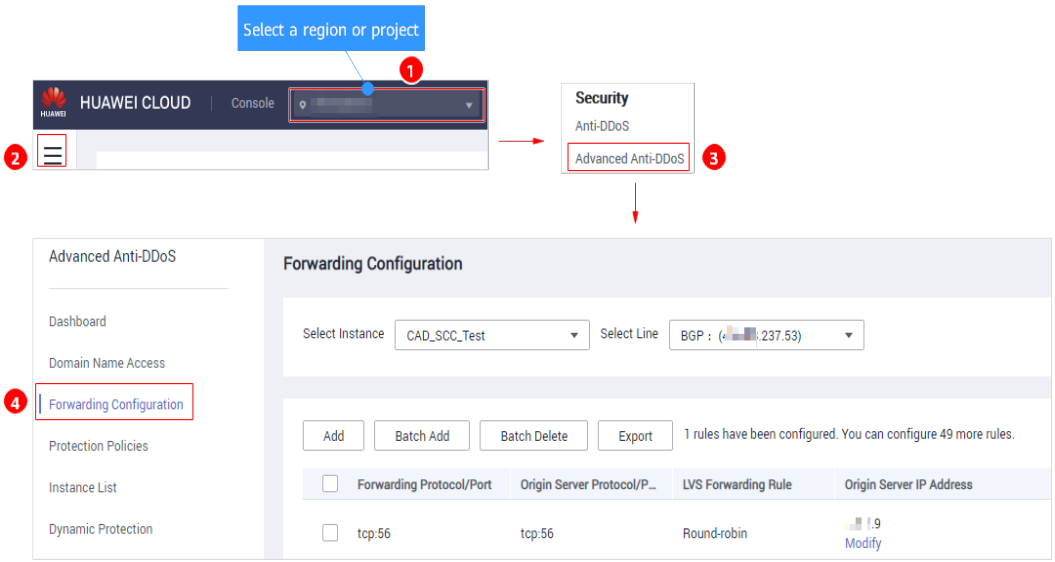
Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-1 Forwarding configuration entry



Step 3 On the **Forwarding Configuration** page, add forwarding rules.

NOTE

- One origin server IP address can be added to multiple forwarding rules.
- The forwarding protocol and forwarding port in each forwarding rule must be unique.
- You can enter a forwarding protocol or port to search for specific rules in the search box in the upper right corner of the page.

- Add a single forwarding rule.
  a. Click **Add** on the **Forwarding Configuration** page.
  b. In the **Add Forwarding Rule** dialog box, configure forwarding rule information and click **OK**. **Table 4-1** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-2 Adding a forwarding rule

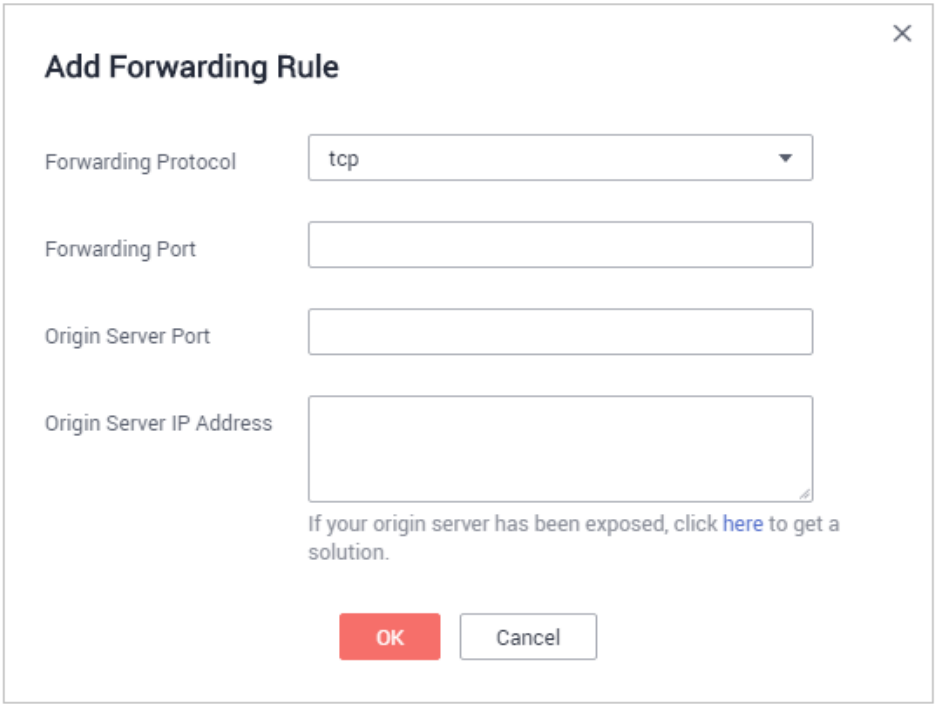


Table 4-1 Parameters for adding a forwarding rule

Parameter	Description
Forwarding Protocol	Specifies the protocol used to forward user service workload. ■ **tcp**: TCP is a connection-oriented protocol that provides reliable delivery of a stream of bytes at the transport layer. ■ **udp**: UDP is a connectionless protocol that provides simple transaction-oriented delivery of messages at the transport layer.
Forwarding Port	Specifies the ingress port used to forward user service workload. The value can be **1** to **65535**. ■ In one line, website services and non-network services cannot use the same port number.
Origin Server Port	Specifies the egress port used to forward user service workload. The value can be **1** to **65535**.

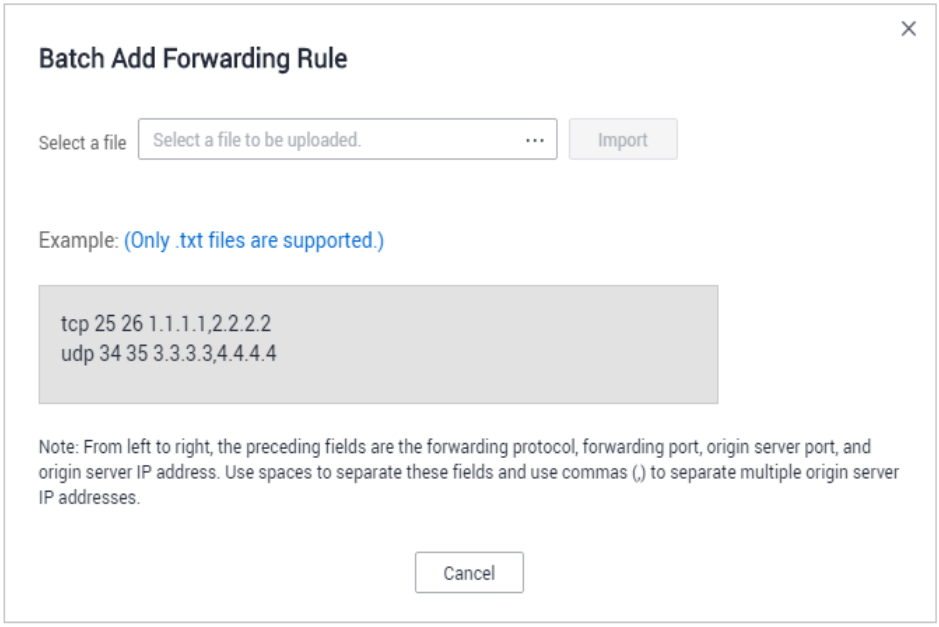
Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Origin Server IP Address	Specifies the public IP address used by the origin server. ■ After configuring the rules, change the domain names based on your services. AAD will automatically forward traffic to your origin server IP addresses. ■ You can add a maximum of 20 origin server IP addresses. Separate them with commas (,). ■ Enter a valid public IP address.

c. Click **OK**.

- Batch add forwarding rules.
  a. Click **Batch Add** on the **Forwarding Configuration** page.
  b. In the **Batch Add Forwarding Rule** dialog box, click ... to select a file and click **Import**.

Figure 4-3 Adding forwarding rules in batches



 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Only a .txt file can be imported.
- In the imported file, fields from left to right are the forwarding protocol, forwarding port, origin server port, and origin server IP address, with spaces in between. Multiple origin server IP addresses are separated using commas (,).
- Each line accommodates only one forwarding rule. **Table 4-1** describes each field.
- The number of forwarding rules in the file cannot exceed the quota limit. Under the quota limit, you can import a maximum of 200 forwarding rules at a time.

----End

Follow-up Procedure

- To change the origin server IP address of a forwarding rule, see **Changing an Origin Server IP Address**.
- If a forwarding rule is not required, delete it by referring to **Deleting a Forwarding Rule**.
- To back up a forwarding rule or quickly modify its configuration information, go to **Exporting a Forwarding Rule**.

 Copyright © Huawei Technologies Co., Ltd.

5 Configuring a Protection Policy

5.1 Configuring a Blacklist and a Whitelist

Scenarios

This section describes how to configure a blacklist and a whitelist for an AAD instance that has added a protected domain name.

Prerequisites

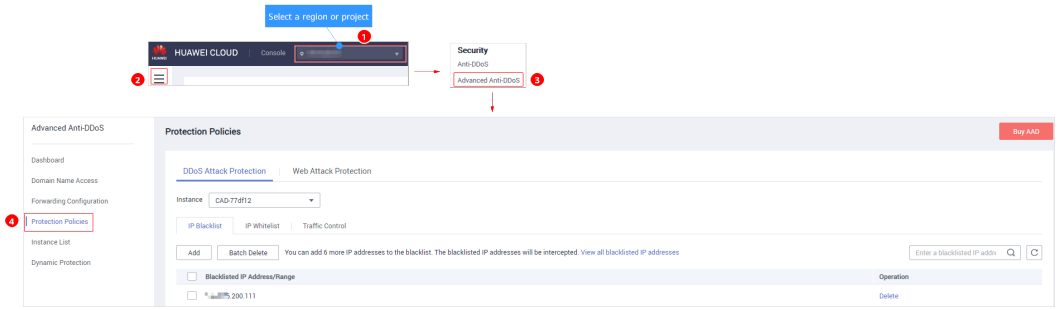
- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Protection Policies** page.

Figure 5-1 Entering the **Protection Policies** page



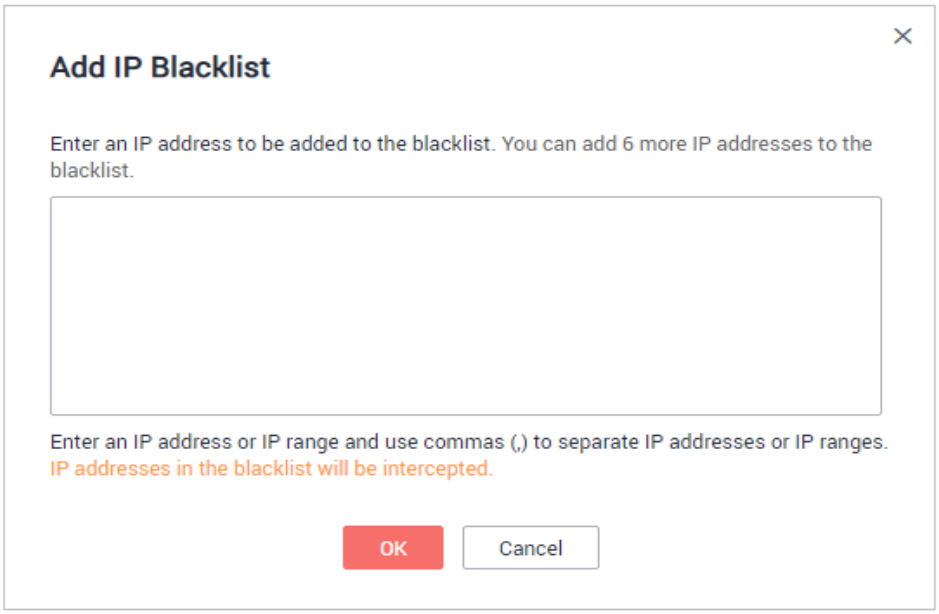
Step 3 In the drop-down list of **Instance**, select the instance for which you want to configure a blacklist or whitelist.

Step 4 Configure a blacklist and a whitelist.

 Copyright © Huawei Technologies Co., Ltd.

- Configuring an IP blacklist
  a. Select the **IP Blacklist** tab and click **Add**.
  b. In the displayed dialog box, enter the IP addresses or IP ranges to be blocked.

     Figure 5-2 Adding blacklisted IP addresses

     NOTE

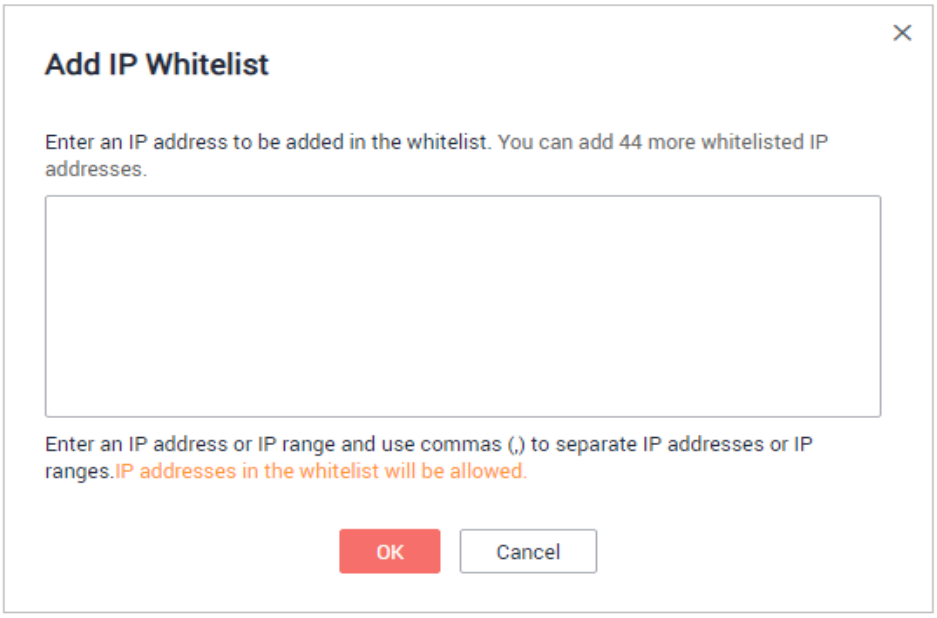
     A maximum of 100 IP addresses can be added to the blacklist of an instance, and IP addresses in the blacklist will be blocked.

  c. Click **OK**.

     On the **IP Blacklist** page, click **Delete** in the **Operation** column or select the blacklisted IP addresses to be deleted and click **Delete** to delete IP addresses in batch. Deleted IP addresses will not be blocked.
- Configuring an IP whitelist
  a. Select the **IP Whitelist** tab and click **Add**.
  b. In the displayed dialog box, enter the IP addresses or IP ranges to be permitted.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-3 Adding whitelisted IP addresses



NOTE

A maximum of 100 IP addresses can be added to the whitelist of an instance. IP addresses in the whitelist are permitted.

c. Click **OK**.

On the **IP Whitelist** page, click **Delete** in the **Operation** column or select the whitelisted IP addresses to be deleted and click **Delete** to delete IP addresses in batch. After an IP address is deleted from the whitelist, the device will not directly permit traffic from this IP address.

----End

5.2 Configuring Traffic Control

Scenarios

This section describes how to perform traffic control on AAD instance lines.

Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

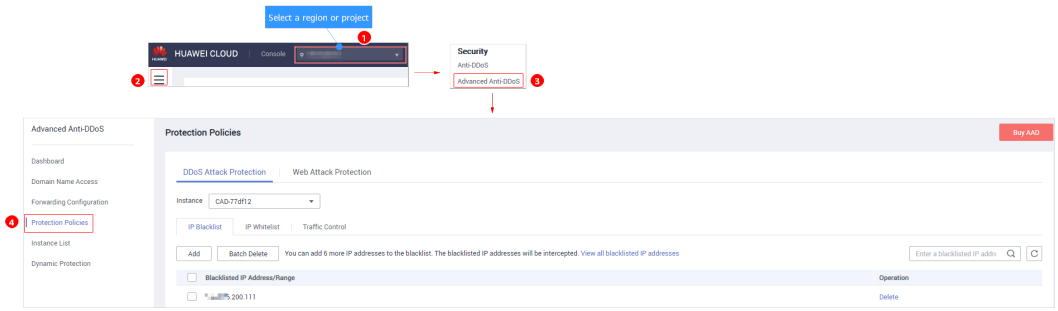
Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Protection Policies** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-4 Entering the **Protection Policies** page



Step 3 In drop-down list of **Instance**, select the instance for which you want to configure traffic control.

Step 4 Click the **Traffic Control** tab to view the status of **Traffic Control Outside Chinese Mainland** and **UDP Traffic Control**.

Figure 5-5 Traffic control

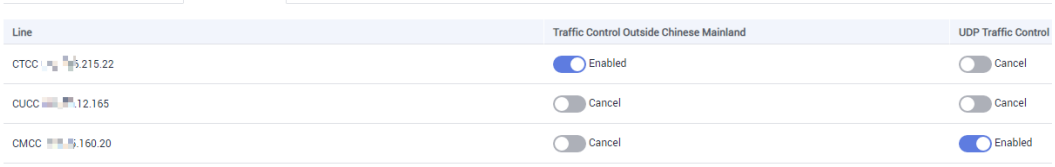


Table 5-1 Parameter description

Parameter	Description
Line	Line and IP address information about an instance
Traffic Control Outside Chinese Mainland	The default value is **disabled**. • If you set this parameter to , traffic outside Chinese mainland will be blocked. • If you set this parameter to , traffic outside Chinese mainland will not be blocked.
UDP Traffic Control	The default value is **disabled**. • If you set this parameter to , UDP traffic will be blocked. • If you set this parameter to , UDP traffic will not be blocked.

----End

 Copyright © Huawei Technologies Co., Ltd.

5.3 Configuring CC Attack Protection Rules

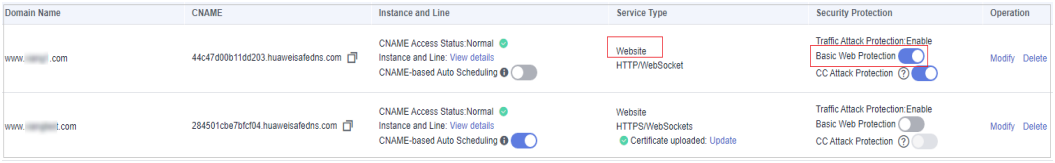
Scenarios

After website services are connected to AAD, you can configure Challenge Collapsar (CC) protection rules to restrict access to a specific URL on your website based on a unique IP address, cookie, or Referer field. AAD can accurately identify CC attacks and effectively mitigate CC attacks based on the protection rules you configured.

Prerequisites

Website services have been connected to AAD and **Basic Web Protection** has been enabled.

Figure 5-6 Basic Web Protection enabled for website services

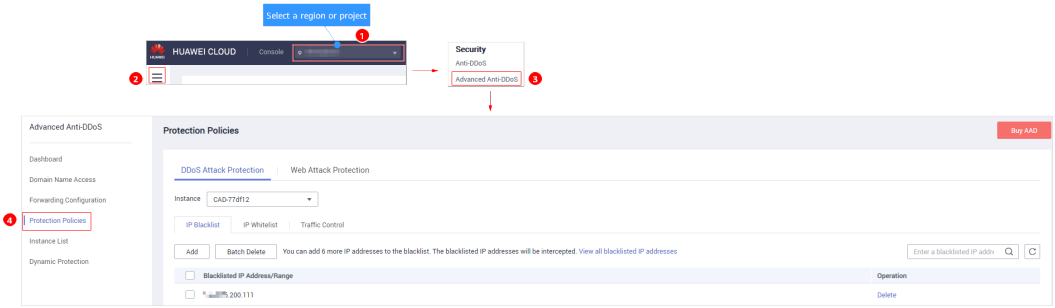


Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Protection Policies** page.

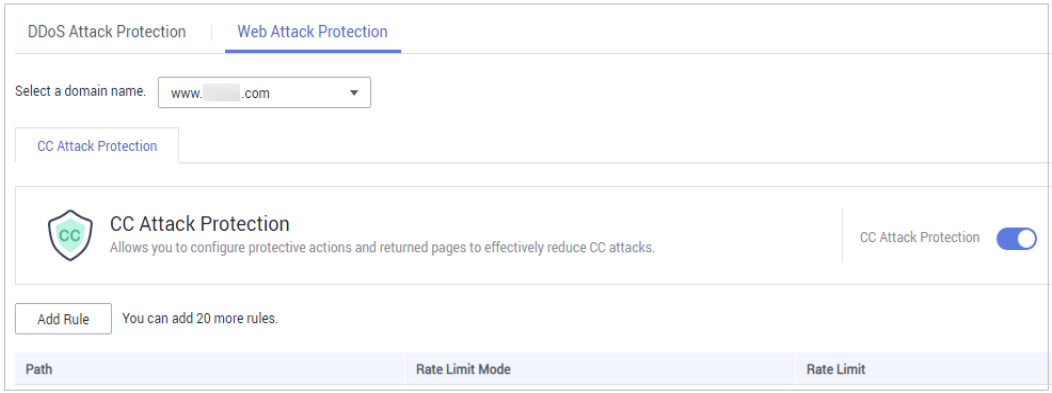
Figure 5-7 Entering the **Protection Policies** page



Step 3 Click the **Web Attack Protection** tab and select the domain name for which you want to configure a protection policy from the **Select a domain name** drop-down list.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-8 Web attack protection



Step 4 Set **CC Attack Protection** to  to enable the protection.

NOTE

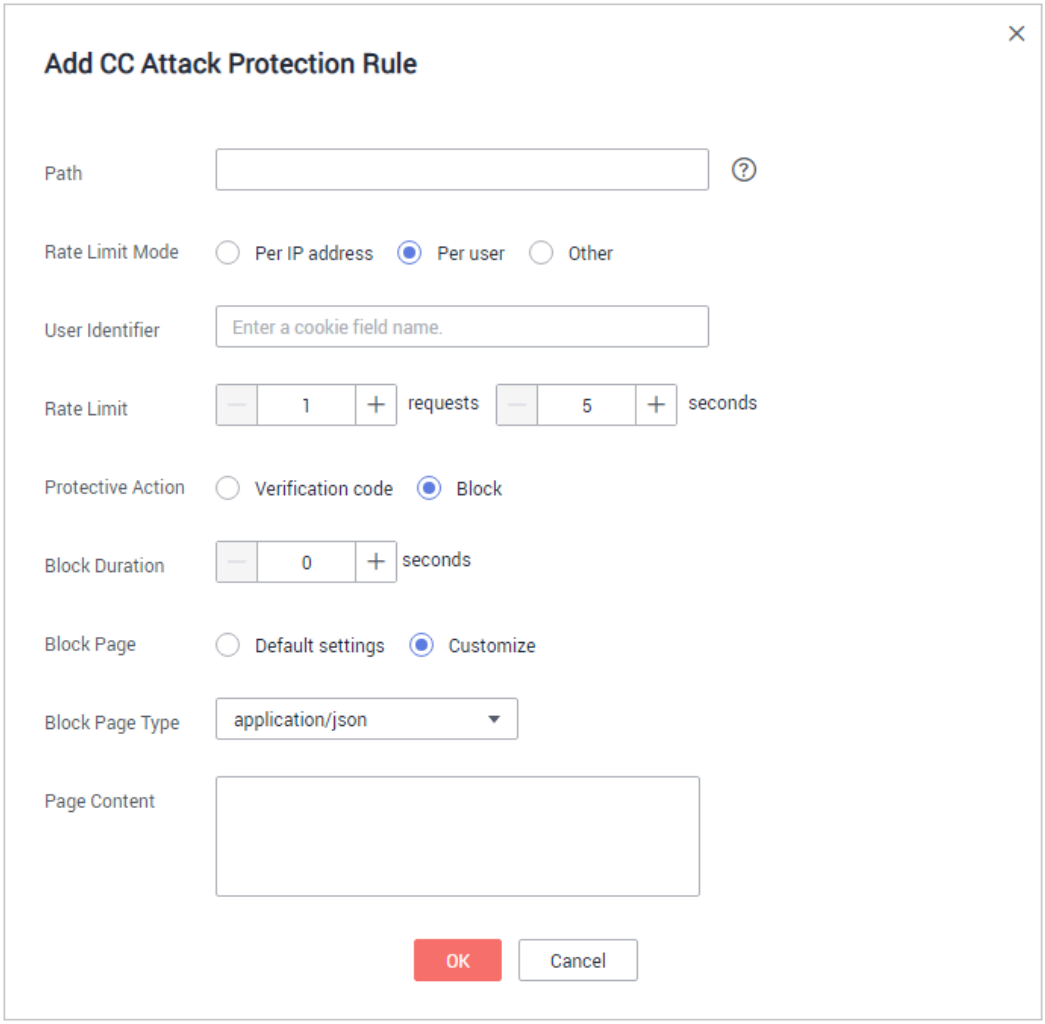
- Traffic Attack Protection is enabled by default.
- Before enabling **CC Attack Protection**, you need to enable **Basic Web Protection**.

Step 5 Click **Add Rule**.

Step 6 In the displayed dialog box, set required parameters. **Table 5-2** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-9 Adding a CC attack protection rule



 Copyright © Huawei Technologies Co., Ltd.

Table 5-2 Parameters for adding a CC attack protection rule

Parameter	Description	Example Value
Path	Specifies the URL to be protected against CC attacks. The value does not contain a domain name. It supports the following matching rules: • Prefix match: Enter a value ending with an asterisk (*), and this value will be used as a prefix in the match. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, you can set **Path** to **/admin***. • Exact match: Enter a value exactly the same as the path to be protected. For example, if the path to be protected is **/admin**, set **Path** to **/admin**. **NOTE** • The path does not support regular expressions. • The path cannot contain two or more consecutive slashes, for example, **///admin**. If you enter **///admin**, the WAF engine converts **///** to **/**.	/admin*

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Rate Limit Mode	• **Per IP address**: A web visitor is identified by the IP address. • **Per user**: A web visitor is identified by the cookie key value. • **Other**: A web visitor is identified by the **Referer** field (user-defined request source). **NOTE** If you set **Rate Limit Mode** to **Other**, enter a complete URL containing the domain name in the **Content** text box for the **referer** field. The **Content** field supports prefix match and exact match only, and cannot contain two or more consecutive slashes, for example, **///admin**. If you enter **///admin**, the WAF engine converts it to **/admin**. For example, if **Path** is **/admin** and you do not want visitors to access the page from **www.test.com**, set **Content** to **http://www.test.com**.	Per user
User Identifier	Specifies an attribute variable in the cookie that uniquely identifies the web visitor. You need to set this parameter if **Rate Limit Mode** is **Per user**. This value supports only the exact match and does not support regular expressions. If you do not set the cookie key value, WAF will automatically assign one. For example, if a website uses the **name** field in the cookie to uniquely identify a web visitor, you can enter the **name** field for **User Identifier**.	name
Rate Limit	Specifies the number of requests allowed from a web visitor in the rate limiting period. Access from the visitor is denied once the limit is reached.	10 requests 60 seconds

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Protective Action	Specifies the action to be taken once the maximum number of requests is reached. Options are **Verification code** and **Block**. • **Verification code**: A verification code is displayed when the number of requests reaches the maximum limit within a specified period. Upon completing the verification, you are no longer restricted by the maximum number of requests allowed. • **Block**: Requests are blocked if the maximum number of requests is reached. **NOTE** If **Rate Limit Mode** is **Other**, **Protective Action** can only be **Block**.	Block
Block Duration	Specifies the period within which access is blocked. An error page is displayed in this period.	600 s
Block Page	Specifies the error page displayed when the maximum number of requests has been reached. This parameter is mandatory only when **Protective Action** is **Block**. Available options are **Default settings** and **Customize**. • If you select **Default settings**, the default block page is displayed. • If you select **Customize**, customize a page to be displayed.	Customize
Block Page Type	Specifies the type of the page you will customize. You can select **application/json**, **text/html**, or **text/xml**.	text/html

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Page Content	Specifies the content to be displayed on the page you will customize.	<html><body>Forbidden</body></html>

Step 7 Click **OK**. The CC attack protection rule is displayed in the CC rule list.

----End

6 Adding a CNAME Record

AAD supports A record-based access and CNAME-based access. CNAME-based access is recommended.

NOTICE

- When adding a CNAME record, you must delete the existing A records from the DNS record set. If they are not deleted, you will fail to add the new record because resolution conflicts may occur. Some DNS service providers support the change from A records into CNAME records, and this change does not affect domain name resolution.
- The DNS configuration may affect current service operating. Therefore, you are advised to configure DNS during off-peak hours.

CNAME-based access has the following advantages:

- Easy to use. You only need to modify the resolution configuration at a time during domain name resolution (for example, on HUAWEI CLOUD DNS).
- Automatic line switchover. If an AAD line encounters an exception, the CNAME resolution can be automatically switched to other properly working lines.
- Service continuity. In a three-line package service, if a line is attacked and blocked by a black hole, AAD automatically uses the other available lines to complete CNAME resolution, ensuring service availability.

The configuration mechanism is similar for each DNS service provider, with small differences in steps. This topic uses the Domain Name Service (DNS) on HUAWEI CLOUD as an example.

Adding a CNAME Record

If you have configured domain name access in **Connecting a Non-website Service to AAD**, you obtain a CNAME record from AAD. Add the CNAME record to DNS.

Step 1 Log in to the management console. Click **Service List**. Under **Network**, click **Domain Name Service**. The **DNS** console is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 In the navigation pane on the left, choose **DNS Resolution** > **Public Zones**. Then click the desired domain name in the list.

Step 3 Click **Add Record Set**.

Step 4 Add the CNAME record. For details, see **Table 6-1**.

Figure 6-1 Adding a record set

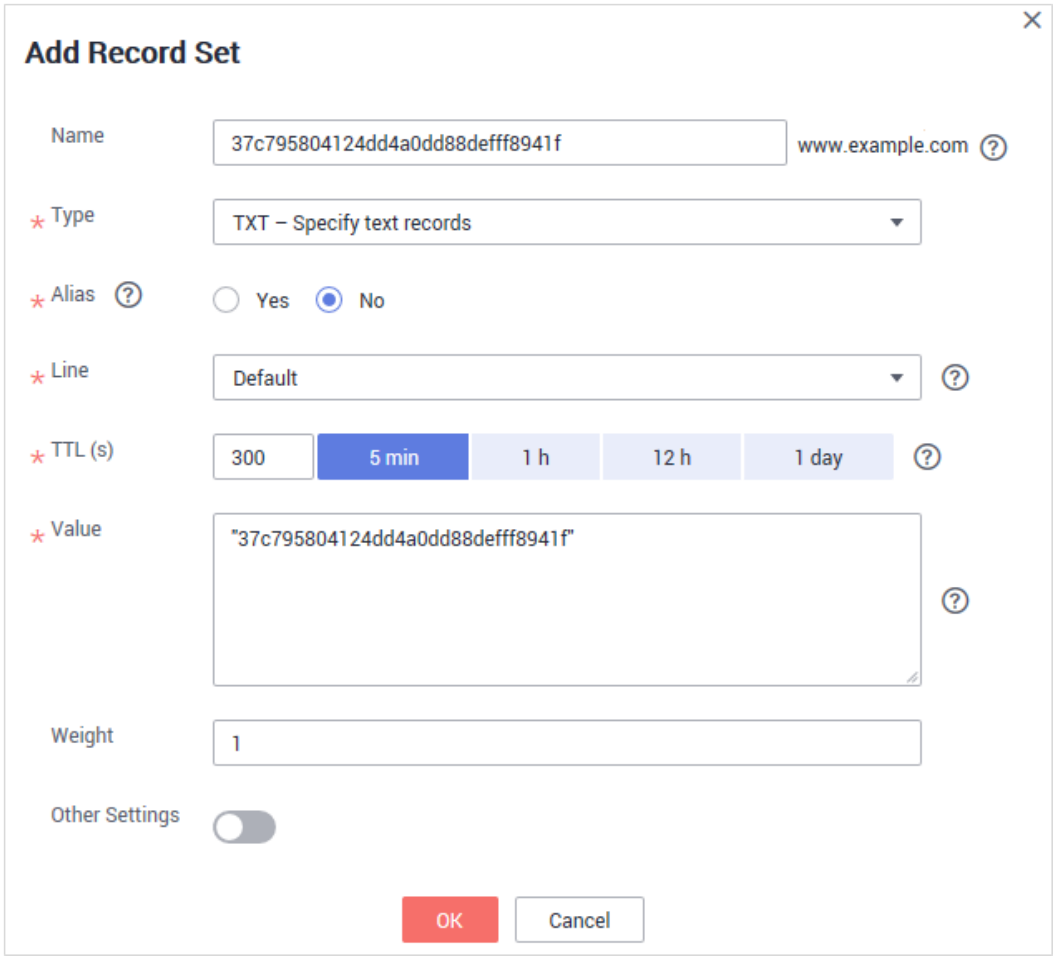


Table 6-1 Parameters for adding a CNAME record

Parameter	Description
Name	Domain name alias (You do not need to manually add the suffix.)
Type	Record set type Select **CNAME – Map one domain to another**.
Alias	Whether to associate the record set with a cloud resource name Select **No**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Line	Resolution line. The DNS server will return the IP address of the specified line based on the source of visitors. Select **Default**.
Value	Domain name mapped to the alias Enter the CNAME record obtained from AAD.

Step 5 Click **OK**.

----End

The DNS configuration takes effect after a period of time. In this period, you can test the domain name resolution using some online test tools such as 17ce and China Webmaster.

Adding an A Record

If you added a forwarding rule without configuring domain name access in **Connecting a Non-website Service to AAD**, add an A record to DNS.

The following steps use the China Telecom line package as an example.

Step 1 Log in to the management console. Click **Service List**. Under **Network**, click **Domain Name Service**. The **DNS** console is displayed.

Step 2 In the navigation pane on the left, choose **DNS Resolution** > **Public Zones**. Then click the desired domain name in the list.

Step 3 Click **Add Record Set**.

Step 4 Add an A record. For details, see **Table 6-2**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Adding an A record set

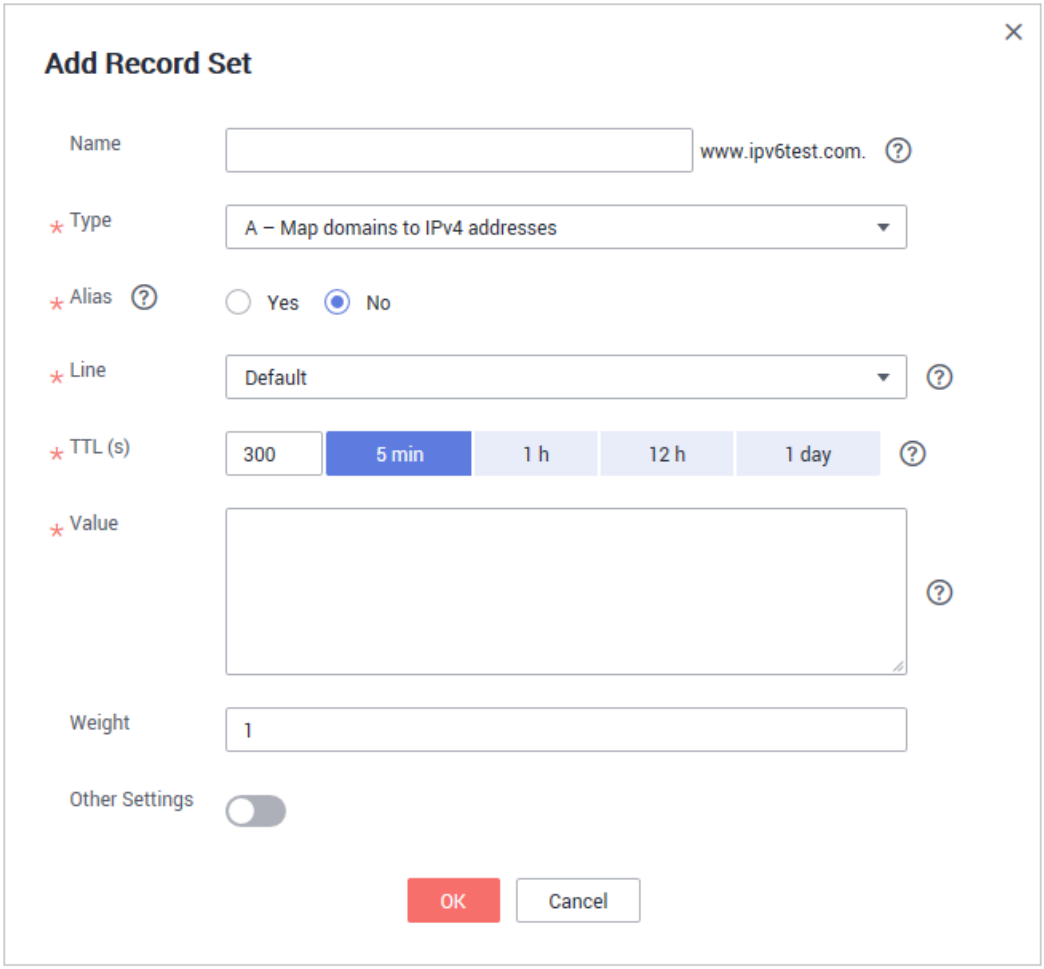


Table 6-2 Parameters for adding an A record - China Telecom

Parameter	Description
Name	Domain name (You do not need to manually add the suffix.)
Type	Record set type Select **A – Map domains to IPv4 addresses**.
Alias	Whether to associate the record set with a cloud resource name Select **No**.
Line	Resolution line. The DNS server will return the IP address of the specified line based on the source of visitors. Select **ISP** and **China Telecom**.
Value	IPv4 addresses mapped to the domain name Enter the high-defense IP address of the China Telecom line.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Click **OK**.

----End

The DNS configuration takes effect after a period of time. In this period, you can test the domain name resolution using some online test tools such as 17ce and China Webmaster.

 Copyright © Huawei Technologies Co., Ltd.

7 Viewing Protection Details

Scenarios

After your services are connected to AAD, you can view the DDoS and CC protection details of different lines in an AAD instance on the dashboard to learn about the current network security state.

On the **Dashboard** page, you can view the following protection details:

- DDoS Attack Protection

  The **Dashboard** page gives an overview of the peak ingress traffic, peak attack traffic, and number of DDoS attacks, and shows the attack type distribution, DDoS attack events, and top 5 attack types scrubbed on two tab pages **Traffic** and **Packet Rate**.

- CC Attack Protection

  The **Dashboard** page gives an overview of number of requests and attacks, attack type distribution, and top 5 attacked source IP addresses.

Precautions

- The protection details cannot be downloaded.
- On the **Dashboard** page, you can view the following protection details of the following time ranges:
  - DDoS Attack Protection

    You can select an AAD instance and a line to view the DDoS protection details of last 24 hours, last 3 days, last 7 days, last 30 days, or a custom period (maximum of last 90 days).
  - CC Attack Protection

    You can select a specific domain name or all domain names from the domain name drop-down list to view the CC protection details of yesterday, today, last 3 days, last 7 days, or last 30 days.

Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

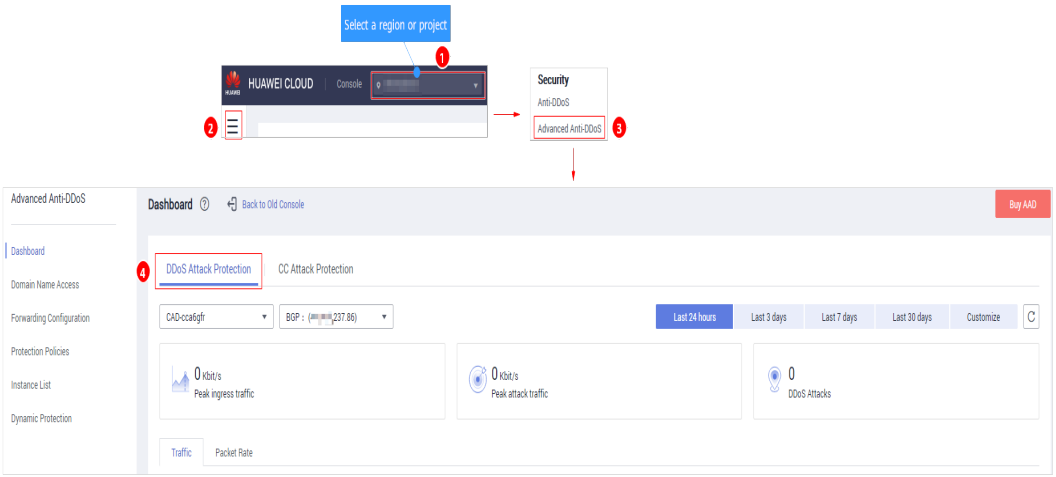
 Copyright © Huawei Technologies Co., Ltd.

Viewing DDoS Attack Protection Details

Step 1 Log in to the management console.

Step 2 Follow the procedure in the following figure to enter the **Advanced Anti-DDoS** console page. In the navigation pane on the left, choose **Dashboard** and then select the **DDoS Attack Protection** tab.

Figure 7-1 DDoS attack protection entry



Step 3 Select an instance, line, and time range (last 24 hours, last 3 days, last 7 days, last 30 days, or a custom period). **Table 7-1** describes the related parameters.

Table 7-1 Parameter description

Parameter	Description
Peak ingress traffic	Maximum traffic accessing the specified IP address of a specified instance per second
Peak attack traffic	Maximum traffic attacking the specified IP address of a specified instance per second
DDoS Attacks	Number of DDoS attacks launched on the specified IP address of a specified instance
Traffic	Trend charts of received traffic and attack traffic
Packet Rate	Trend charts of received packets and attack packets

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Attack Type Distribution	Types of attack events • You can click any colored area in the attack distribution circle under **Attack Type Distribution** to view the type, count, and proportion of an attack. • To stop displaying information about a specific type of attacks, click the legend with the same color to the right of the circle.
Top 5 Attack Types Scrubbed (Kbit/s)	Top 5 attack types that have been scrubbed
DDoS Attack Events	Details about DDoS attacks

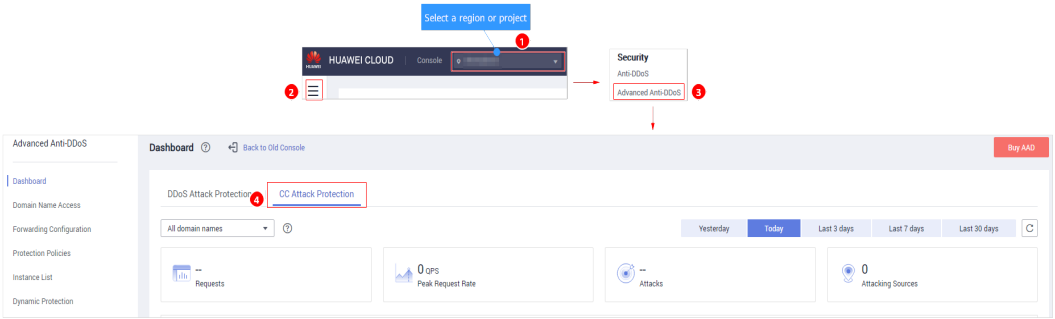
----End

Viewing CC Attack Protection Details

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Advanced Anti-DDoS** console page. In the navigation pane on the left, choose **Dashboard** and then select the **CC Attack Protection** tab.

Figure 7-2 CC attack protection entry



Step 3 Select the target domain name from the **All domain names** drop-down list (select one domain name or retain all domain names).

In the upper right corner of the page, select a time range (yesterday, today, last 3 days, last 7 days, or last 30 days). **Table 7-2** describes the related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 7-2 Parameter description

Parameter	Description
Requests	Total number of requests to a specified domain name If you select **All domain names**, the total number of requests to all domain names with WAF enabled is collected.
Peak Request Rate	Maximum number of requests to a specified domain name per second If you select **All domain names**, the maximum number of requests to all domain names with WAF enabled is collected per second.
Attacks	Number of attacks towards a specified domain name
Attacking Sources	Number of sources that attack a specified domain name
Request Statistics	• Requests: trend chart for the access requests • Attacks: trend chart for attacks
Attack Type Distribution	Types of attack events • You can click any colored area in the attack distribution circle under **Attack Type Distribution** to view the type, count, and proportion of an attack. • To stop displaying information about a specific type of attacks, click the legend with the same color to the right of the circle.
Top 5 Attacking Source IP Addresses	Top 5 attacking source IP addresses and their cumulative number of attacks

----End

 Copyright © Huawei Technologies Co., Ltd.

8 Enabling Alarm Notification

After you enable the alarm notification, a notification message will be sent to you through the method you have configured when:

- The IP address is under the DDoS attacks.
- The additional fees are incurred for the traffic exceeds the basic protection bandwidth threshold.

  You will receive an alarm notification in the morning of the next day.

Precautions

- The Simple Message Notification (SMN) service is a paid service. For details about the price, see **SMN Product Pricing Details**.
- Before setting alarm notification, you are advised to create a message topic in the SMN service as an administrator. For details, see **Publishing a Message**.

Prerequisites

You have purchased an AAD instance.

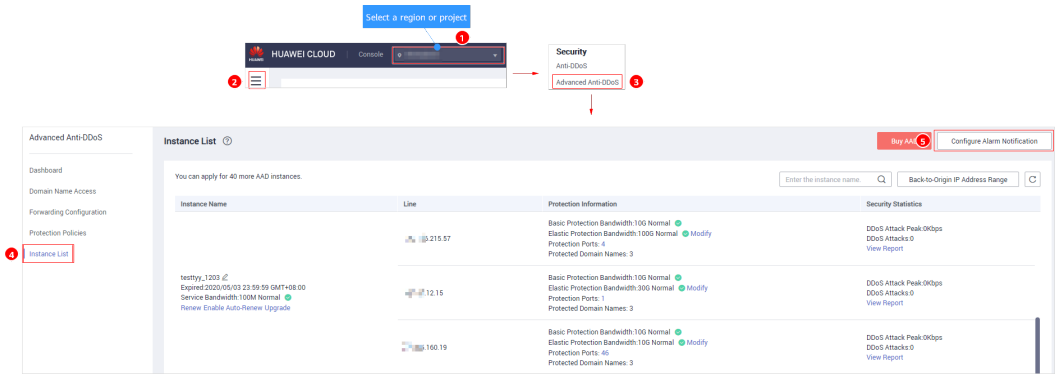
Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Advanced Anti-DDoS** console page. In the navigation pane on the left, choose **Instance List** and then click **Configure Alarm Notification** in the upper right corner.

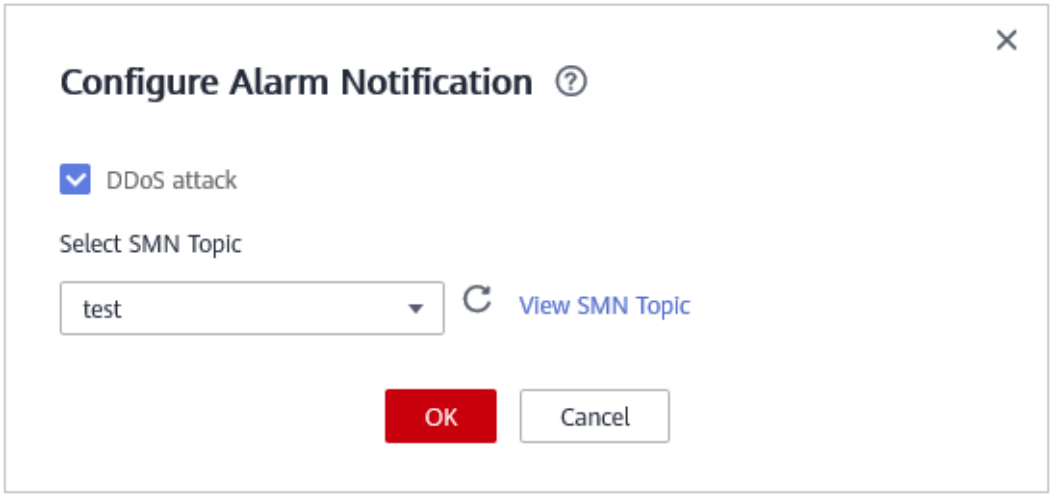
 Copyright © Huawei Technologies Co., Ltd.

Figure 8-1 Alarm notification setting entry



Step 3 In the displayed **Configure Alarm Notification** dialog box, select **DDoS attack**.

Figure 8-2 Configure Alarm Notification



Select an existing topic from the drop-down list or click **View SMN Topic** and create an SMN topic on the displayed page for configuring the terminals for receiving alarm notifications.

Perform the following steps to create a topic:

1. Create a topic by referring to **Creating a Topic**.
2. You can add one or more subscriptions to a topic by configuring the phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**.
3. Confirm the subscription. After the subscription is added, confirm the subscription.

For details about topics and subscriptions, see *Simple Message Notification User Guide*.

Step 4 Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

To disable the alarm notification function, deselect **DDoS attack** in **Figure 8-2** and click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

9 Managing an Instance

9.1 Viewing Information About an Instance

Scenarios

This section describes how to view information about an Advanced Anti-DDoS instance.

Prerequisites

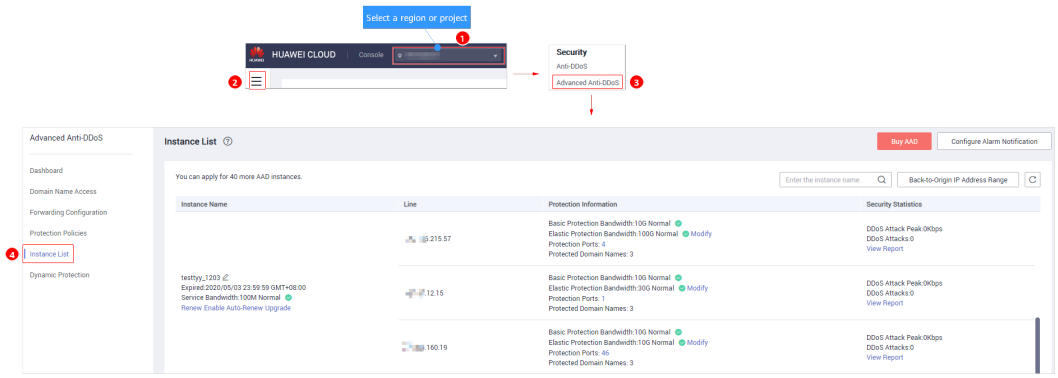
- You have obtained an account and its password to log in to the management console.
- You have purchased an AAD instance.

Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Advanced Anti-DDoS** console page. In the navigation pane on the left, choose **Instance List**.

Figure 9-1 Instance list entry



Step 3 On the displayed page, view the details about an instance. **Table 9-1** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 9-1 Parameter description

Parameter	Description
Instance Name	• Name of an AAD instance. You can click on the right to change the name. • Time when the instance expires • **Recharge** button of the instance • Service bandwidth and protection bandwidth statuses of the instance
Line	Line and IP address information about an instance
Protection Information	Basic protection bandwidth, elastic protection bandwidth, number of protection ports, and number of protected domain names of the instance **NOTE** To change the elastic protection bandwidth, click **Edit**.
Security Statistics	Protection statistics about the instance, including: • Peak attack traffic • Number of attacks
Operation	• Click **View Report** to view the normal traffic and attack traffic. • Click **Configure** to configure forwarding rules for the instance.

----End

9.2 Changing the Name of an AAD Instance

Scenarios

This section describes how to change an AAD instance name.

Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

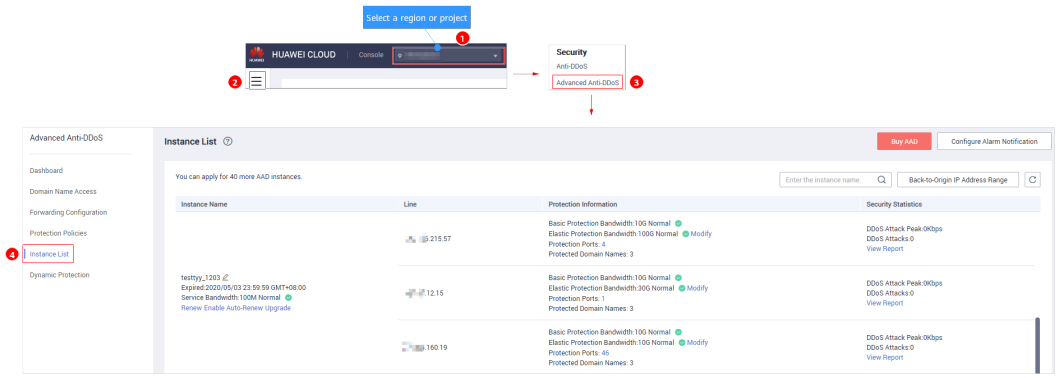
Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Advanced Anti-DDoS** console page. In the navigation pane on the left, choose **Instance List**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-2 Instance list entry



Step 3 In the row containing the desired instance, click next to the instance name.

Step 4 Enter a new instance name in the text box and click .

----End

9.3 Changing the Elastic Protection Bandwidth

Scenarios

You can change the elastic protection bandwidth if it is insufficient.

This section describes how to change the elastic protection bandwidth for an AAD instance.

NOTICE

The elastic protection bandwidth of each instance can be changed for up to three times per day.

Prerequisites

- You have obtained a username and password for logging in to the management console.
- You have purchased an AAD instance.

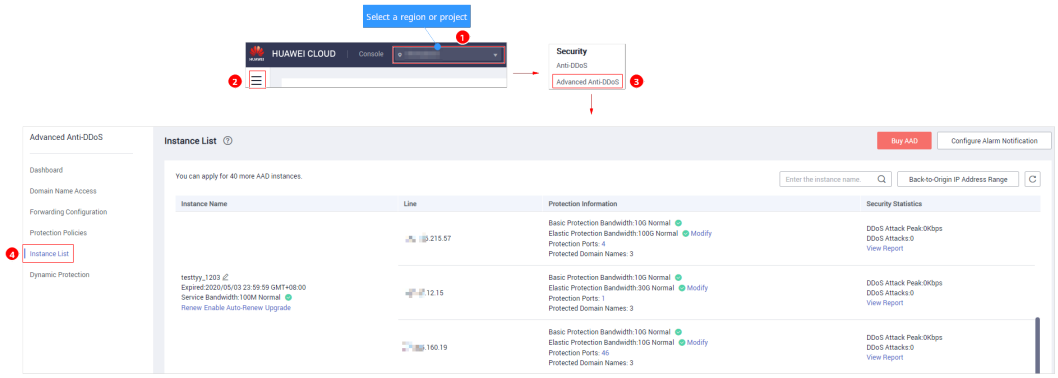
Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Advanced Anti-DDoS** console page. In the navigation pane on the left, choose **Instance List**.

 Copyright © Huawei Technologies Co., Ltd.

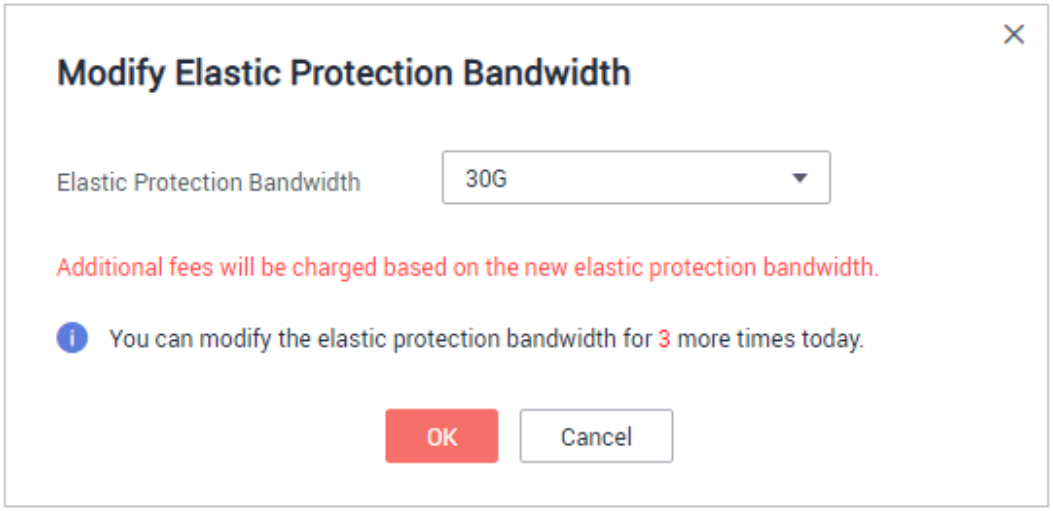
Figure 9-3 Instance list entry



Step 3 In the **Protection Information** column of the row containing the desired instance, click **Edit**.

Step 4 In the dialog box that is displayed, set a new bandwidth and click **OK**.

Figure 9-4 Dialog box for modifying elastic protection bandwidth



----End

 Copyright © Huawei Technologies Co., Ltd.

10 Managing a Forwarding Rule

10.1 Viewing Information About a Forwarding Rule

Scenarios

This topic describes how to view information about a forwarding rule.

Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have configured forwarding rules for AAD instances.

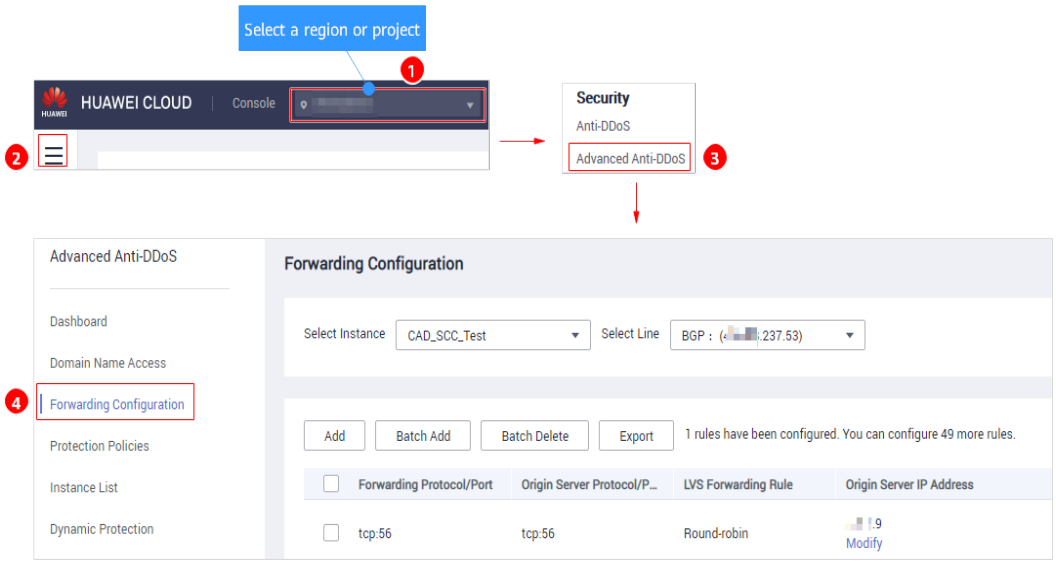
Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-1 Forwarding configuration entry



Step 3 View information about the desired forwarding rule.

Table 10-1 Parameter description

Parameter	Description
Forwarding Protocol/Port	Forwarding protocol and port for the rule
Origin Server Protocol/Port	Origin server protocol and port for the rule
LVS Forwarding Rule	Forwarding rule of the Linux Virtual Server (LVS)
Origin Server IP Address	Origin server IP address added to the rule Click **Modify** if you need to change the origin server IP address.
Status	• Running status of the forwarding rule
Operation	You can click **Delete** to delete the forwarding rule.

----End

10.2 Changing an Origin Server IP Address

Scenarios

You can change the origin server IP address in the forwarding rule whenever necessary during defense.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

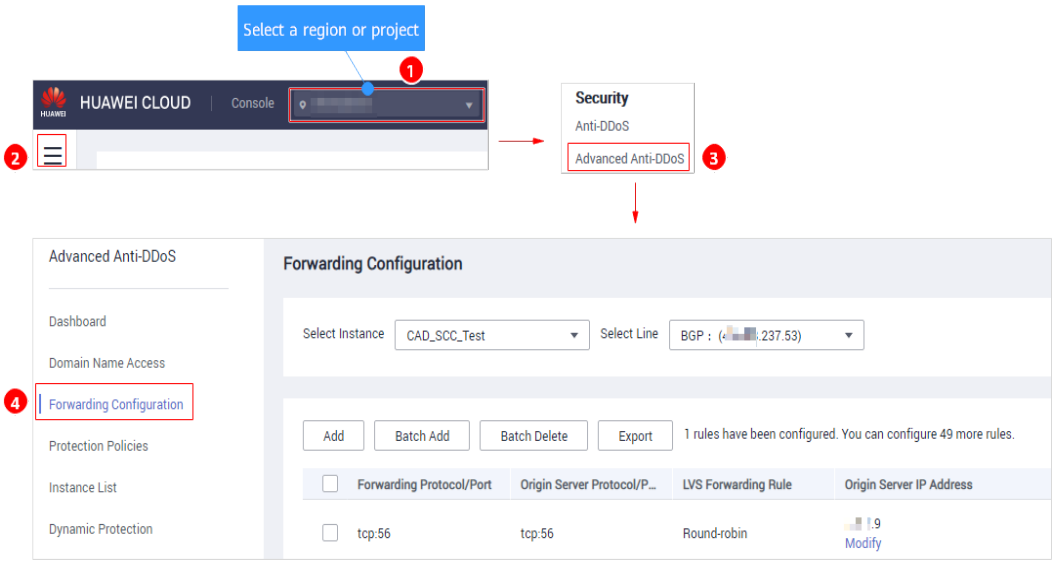
- You have obtained the username and password for logging in to the management console.
- You have configured forwarding rules for AAD instances.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

Figure 10-2 Forwarding configuration entry



Step 3 Locate the row containing the target forwarding rule and click **Modify** in the **Origin Server IP Address** column.

Step 4 In the displayed **Modify Origin Server IP Address** dialog box, change the IP address of the origin server for the forwarding rule.

NOTICE

Enter a valid public IP address.

Step 5 Click **OK**.

----End

10.3 Deleting a Forwarding Rule

Scenarios

You can delete a specific forwarding rule if it is unnecessary.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

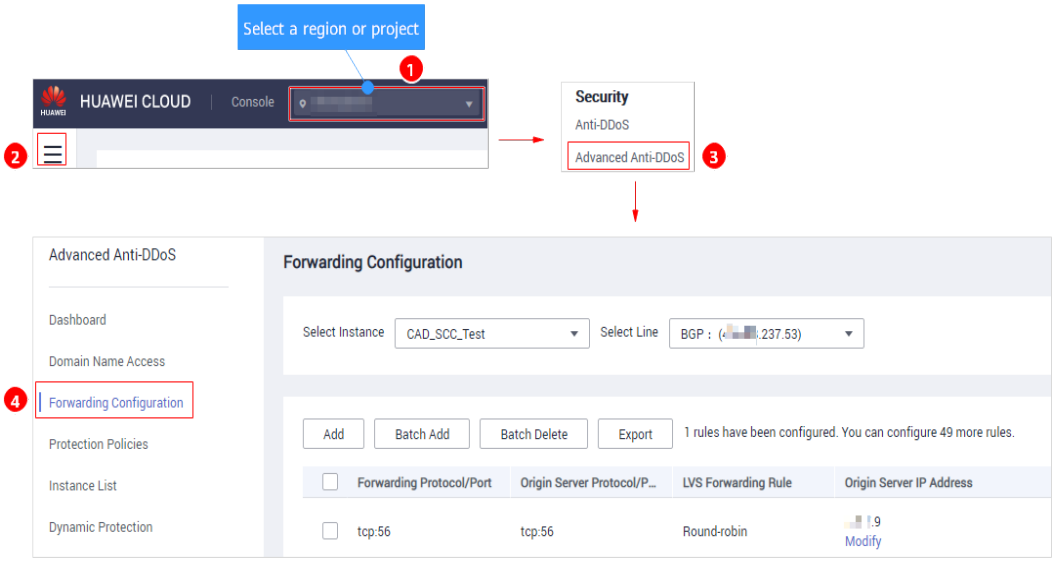
- You have obtained the username and password for logging in to the management console.
- You have configured forwarding rules for AAD instances.

Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

Figure 10-3 Forwarding configuration entry



Step 3 Delete forwarding rules.

- Deleting one forwarding rule
  a. Locate the row containing the target forwarding rule and click **Delete** in the **Operation** column.
  b. Click **OK** in the displayed dialog box.
- Deleting multiple forwarding rules
  a. Select the target forwarding rules and click **Delete** above the forwarding rule list.

  NOTE

  You can batch delete a maximum of 50 forwarding rules at a time. (Up to 50 forwarding rules can be displayed per page.)

  b. Click **OK** in the displayed dialog box.

----End

 Copyright © Huawei Technologies Co., Ltd.

10.4 Exporting a Forwarding Rule

Scenarios

- Back up all forwarding rules of an instance by exporting them.
- Using the exported file, modify forwarding rules quickly and batch add them to the console.

Prerequisites

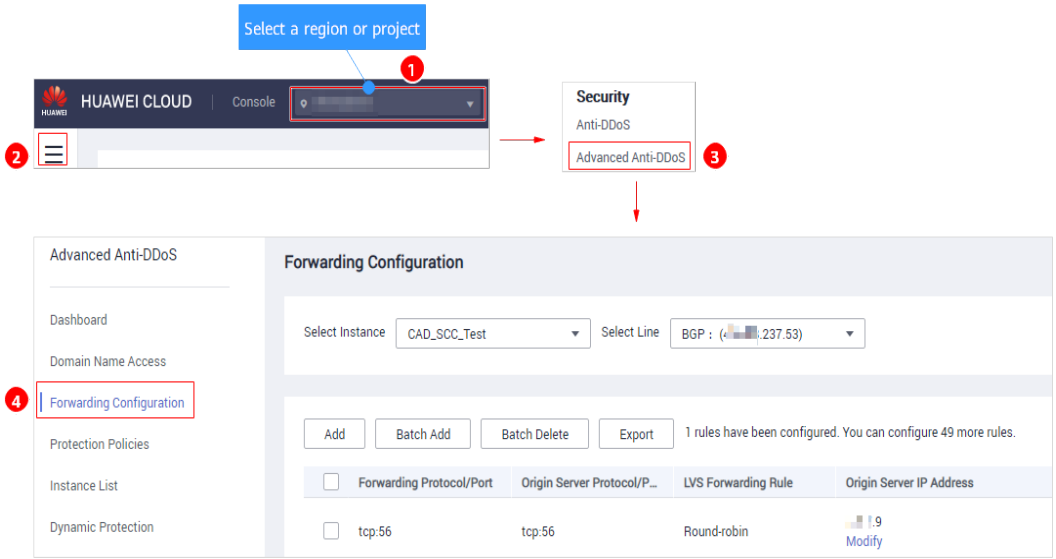
- You have obtained the username and password for logging in to the management console.
- You have configured forwarding rules for AAD instances.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

Figure 10-4 Forwarding configuration entry



Step 3 Click **Export** to export all forwarding rules to the local computer.

Step 4 View the file of exported forwarding rules **rules.txt**.

----End

 Copyright © Huawei Technologies Co., Ltd.

11 Managing a Domain Name

11.1 Viewing Information About a Domain Name

Scenarios

This topic describes how to view information about a domain name.

Prerequisites

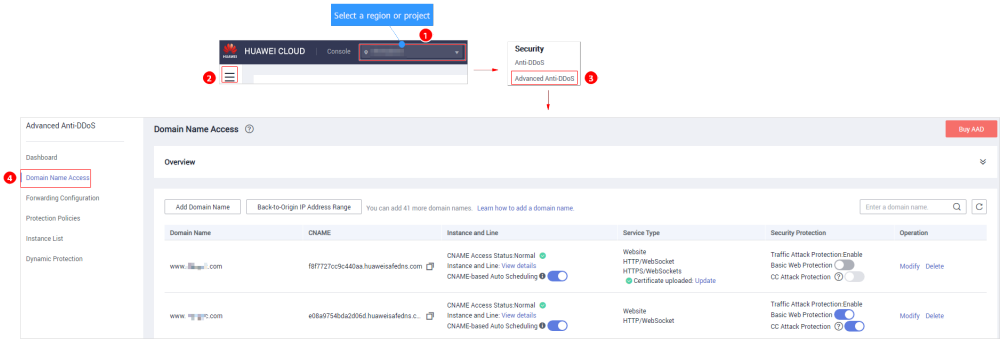
At least one domain name has been added for protection.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure shown in the following figure to enter the **Domain Name Access** page.

Figure 11-1 Domain Name Access page



Step 3 View information about the domain name.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-1 Parameter description

Parameter	Description
Domain Name	Protected domain name
CNAME	• CNAME record obtained for the domain name after a CNAME resolution • Click  to copy the CNAME record.
Instance and Line	• CNAME-based access status of the domain name • Click **View details** to view details about the line of the domain name. • Enable **CNAME-based Auto Scheduling** so that DNS resolution will automatically schedule the traffic if the high-defense IP address is blocked by a black hole.
Service Type	• Service type of the domain name • Locate the row that contains **HTTPS/WebSockets** certificate, click **Update** in the **Service Type** column to update the certificate. For details, see **Updating a Certificate**.
Security Protection	Status of traffic attack protection, basic web protection, and CC attack protection • For a website service whose **Origin Server Type** is set to **IP address**, you can enable basic web protection and CC attack protection for your domain name. • For a website service whose **Origin Server Type** is set to **Domain name**, you do not need to enable basic web protection and CC attack protection for your domain name. • For a non-website service, only traffic attack defense is provided and enabled by default.
Operation	• You can click **Modify** to modify the domain name access configuration. • You can click **Delete** to delete a domain name.

----End

11.2 Enabling Basic Web Protection and CC Attack Protection

Scenarios

After adding a domain name, you can enable **Basic Web Protection** and **CC Attack Protection** for it. Basic web protection and CC attack protection are

 Copyright © Huawei Technologies Co., Ltd.

provided only for the forwarding rules whose **Service Type** is **Website** and **Origin Server Type** is **IP address**.

Prerequisites

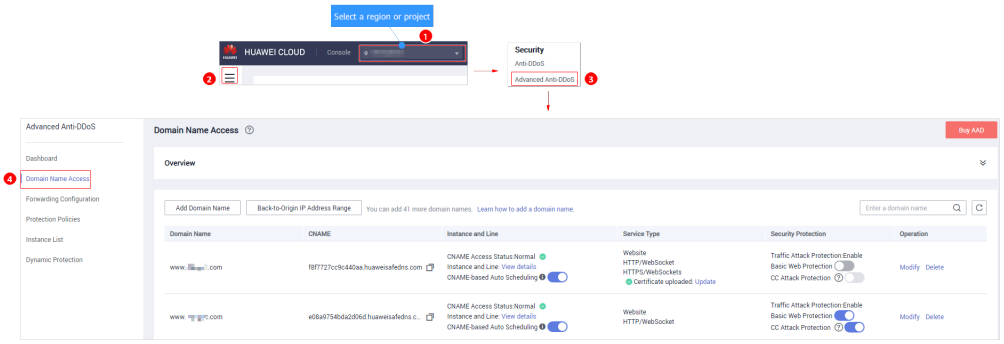
At least one domain name has been added for protection.

Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure shown in the following figure to enter the **Domain Name Access** page.

Figure 11-2 Domain Name Access page



Step 3 Set **CC Attack Protection** to  to enable the WAF protection and CC attack protection.

NOTE

- Basic web protection and CC attack protection are provided only for the forwarding rules whose **Service Type** is **Website** and **Origin Server Type** is **IP address**.
- Traffic attack protection is enabled by default.
- Before enabling CC attack protection, you need to enable basic web protection.

----End

11.3 Updating a Certificate

For website services connected to AAD, if **Protocol/Port** is set to **HTTPS/WebSockets** and **Origin Server Type** is set to **IP address**, you need to upload a certificate (only TLS 1.0, TLS 1.1, and TLS 1.2 certificates are supported) to associate the certificate with the protected domain name.

- If the purchased certificate is about to expire, you are advised to purchase a new certificate before the expiration date and update the certificate associated with the domain name in AAD.
- To update the certificate associated with a domain name, you can associate a new certificate with the domain name in AAD.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

- The certificate takes effect 1 minute after it is updated. Therefore, update certificates in off-peak hours.
- If a certificate expires, the origin server will be affected more severely than the host crash and website access failure. Therefore, you are advised to update the certificate before the certificate expires.
- Each domain name must be associated with a certificate. A wildcard domain name can only be used for a wildcard domain certificate. If you have not purchased a wildcard domain certificate and have only a single-domain certificate, you can only add domain names one by one in AAD.

Prerequisites

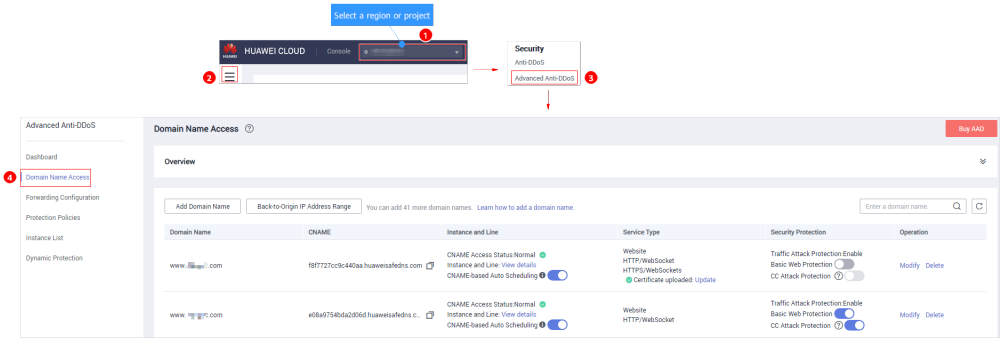
Website services have been connected to AAD.

Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure shown in the following figure to enter the **Domain Name Access** page.

Figure 11-3 Domain Name Access page



Step 3 Locate the row that contains the target domain name, and click **Update** in the **Service Type** column.

Step 4 In the displayed **Update Certificate** dialog box, upload a new certificate or select an existing certificate.

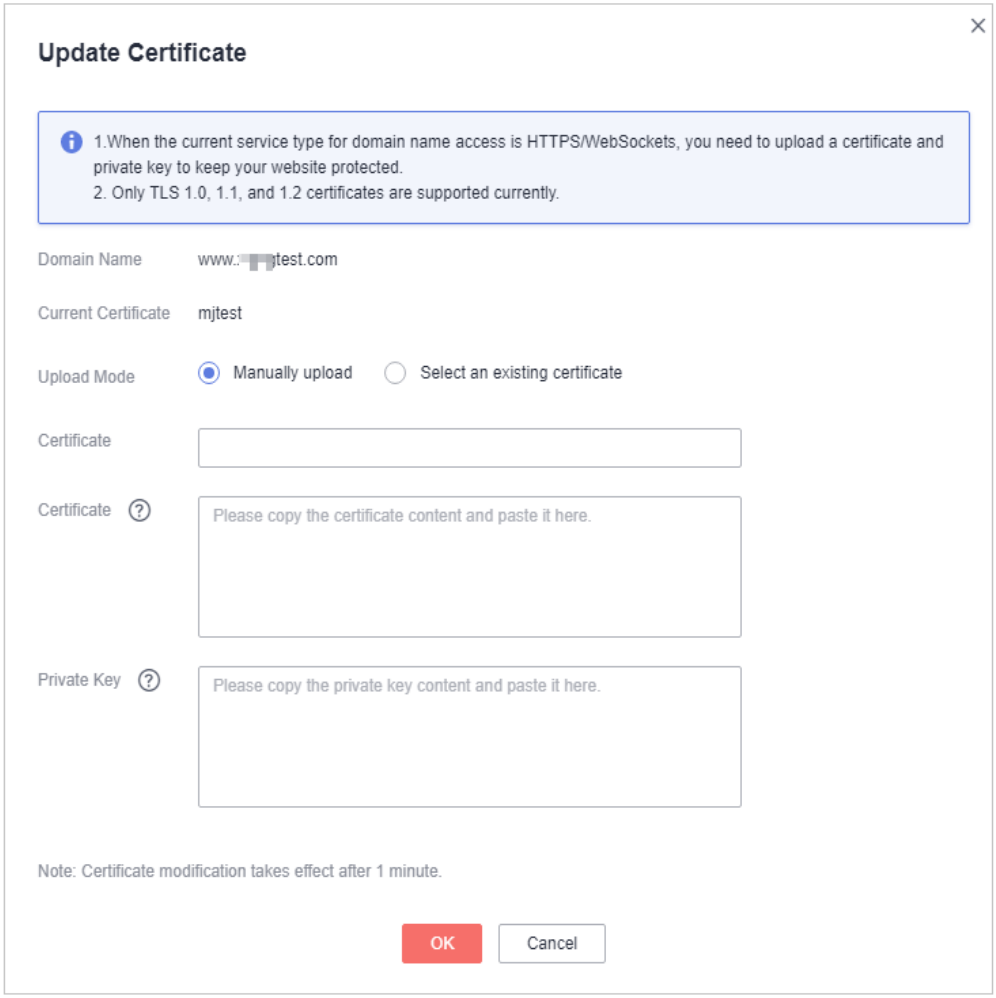
- If **Upload Mode** is set to **Manually upload**, enter the certificate name and paste the certificate content and private key to the target text box, as shown in **Figure 11-4**.

  NOTE

  AAD encrypts and saves the private key file to ensure its security.

 Copyright © Huawei Technologies Co., Ltd.

Figure 11-4 Manually uploading a certificate



Currently, AAD only supports PEM certificates. If the certificate is not in .pem format, convert it into a .pem certificate by referring to **Table 11-2** before uploading.

Table 11-2 Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	Use OpenSSL to convert the certificate. Obtain a private key. For example, run the following command to convert **cert.pfx** into **cert.key**: **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes** Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**

Copyright © Huawei Technologies Co., Ltd.

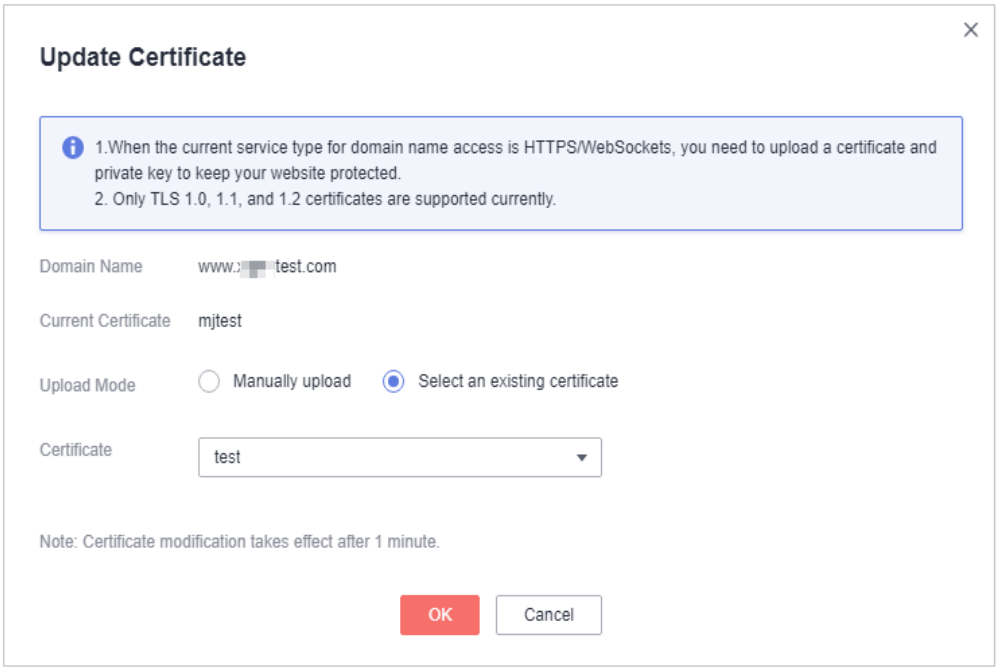
Format	Conversion Method
P7B	Use OpenSSL to convert the certificate. 1. Run the following command to convert the certificate: **openssl pkcs7 -print_certs -in incertificat.p7b -out cert.cer** 2. Obtain the certificate content in **cert.cer**. 3. Save the content in .pem format.
DER	Use OpenSSL to convert the certificate. 1. Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** 2. Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

Before running the openssl command in Windows, ensure that the **openssl** tool has been installed.

- If **Upload Mode** is set to **Select an existing certificate**, select the uploaded certificate from the **Certificate** drop-down list.

Figure 11-5 Selecting an existing certificate



 Copyright © Huawei Technologies Co., Ltd.

Step 5 Click **OK**.

----End

11.4 Modifying Resolution Lines for High-Defense IP Addresses of a Domain Name

Scenarios

This topic describes how to:

- Disable DNS resolution for a high-defense IP address.
- Add a resolution line for a domain name.
- Delete a resolution line for a domain name.

Precautions

The modified resolutions lines take effect in about five minutes.

Prerequisites

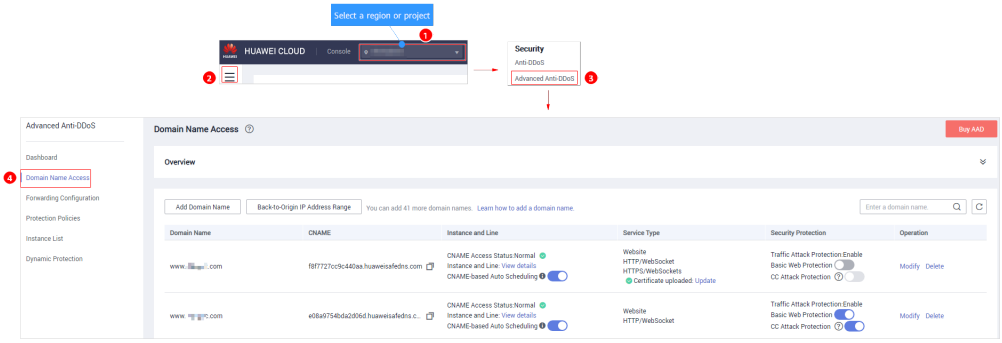
At least one domain name has been added for protection.

Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure shown in the following figure to enter the **Domain Name Access** page.

Figure 11-6 Domain Name Access page



Step 3 In the row containing the desired domain name, click **View details** in the **Instance and Line** column.

Step 4 Modify the resolution lines for the domain name.

- Disable DNS resolution for a high-defense IP address of the domain name.

  On the details page of the domain name, locate the target line and set **DNS Resolution** to  to disable DNS resolution for the high-defense IP address. After you disable DNS resolution, you can still use the A record for the high-defense IP address.

 Copyright © Huawei Technologies Co., Ltd.

- Add a resolution line for the domain name.
  a. On the details page of the domain name, click **Add Line**.
  b. In the **Add Line** dialog box, select new instances and lines and click **OK**.
  c. Set **DNS Resolution** to  to enable DNS resolution for the high-defense IP addresses.
- Delete a resolution line for the domain name.
  a. Disable DNS resolution for the high-defense IP address. For details, see **Disabling DNS Resolution**.
  b. Click **Delete Line**.
  c. Click **OK**.

----End

11.5 Modifying Domain Name Configuration

Scenarios

This topic describes how to modify the domain name configuration of a website service.

Prerequisites

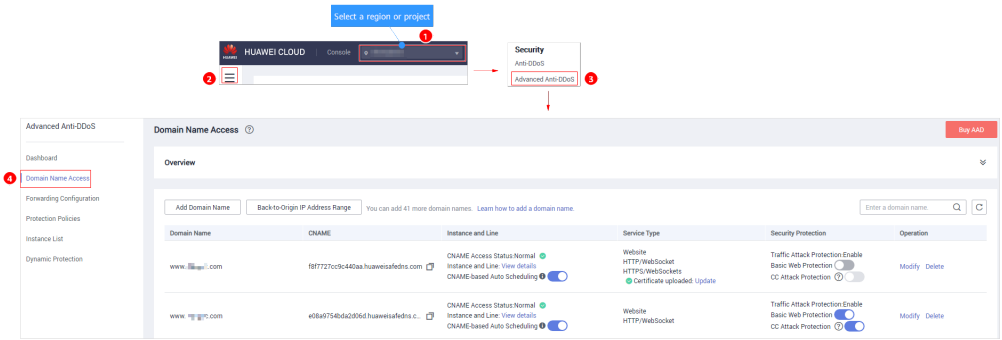
A website service domain name has been added.

Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure shown in the following figure to enter the **Domain Name Access** page.

Figure 11-7 Domain Name Access page



Step 3 In the row containing the desired domain name, click **Modify** in the **Operation** column.

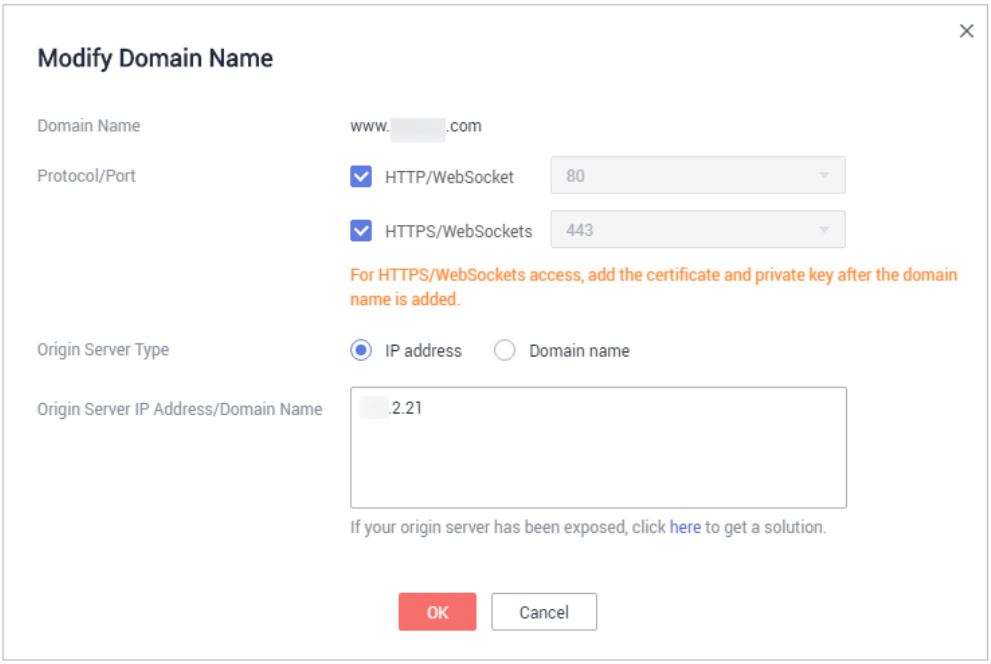
Step 4 In the **Modify Domain Name** dialog box that is displayed, modify the domain name configurations.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If this protected domain name will share a high-defense IP address and port with another domain name, ensure that they have the same **Origin Server Type** value.
- To change the **Origin Server Type** value from **IP address** to **Domain name**, ensure that **Basic Web Protection** is disabled for the domain name.

Figure 11-8 Modifying domain name configurations



Step 5 Click **OK**.

----End

11.6 Deleting a Domain Name

Scenarios

You can delete domain names that you do not want to protect.

NOTICE

Before deleting a domain name, you need to ensure that the DNS domain name provider has changed the CNAME record to the real IP address. Otherwise, deleting the domain name will lead to service unavailability.

Prerequisites

At least one domain name has been added for protection.

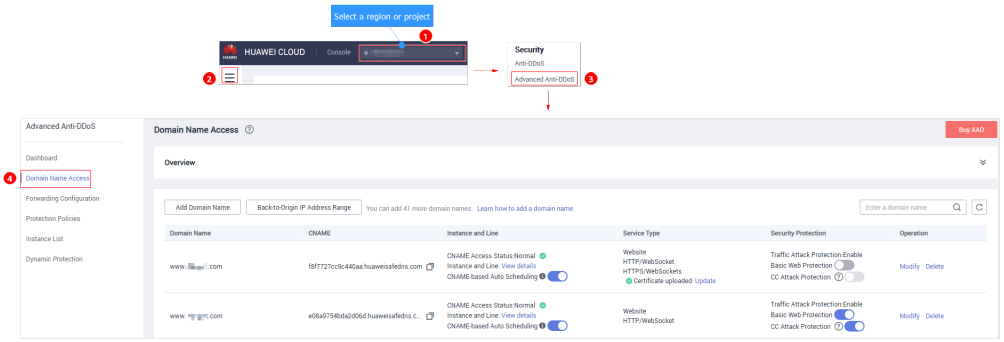
 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure shown in the following figure to enter the **Domain Name Access** page.

Figure 11-9 Domain Name Access page



Step 3 Locate the row containing the target domain name and click **Delete** in the **Operation** column.

Step 4 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

12 Viewing a Back-to-Origin IP Address Range

Scenarios

If a firewall has been configured for your origin server, add the back-to-origin IP address range to the whitelist of the firewall (or another protective software) of the origin server.

This topic describes how to view a back-to-origin IP address range.

Prerequisites

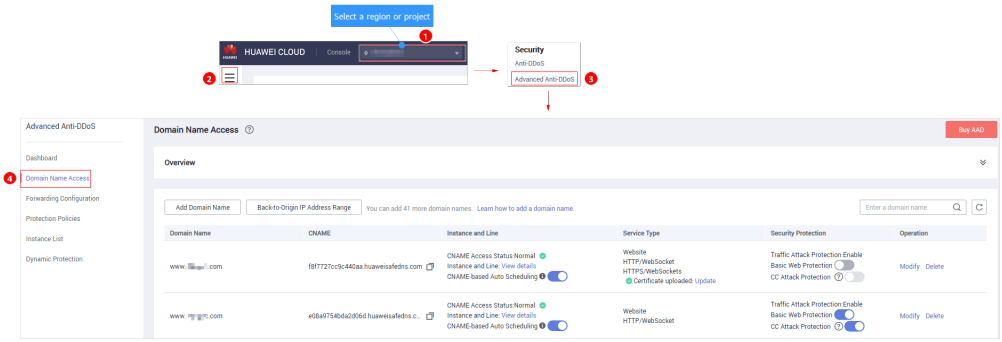
- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure shown in the following figure to enter the **Domain Name Access** page.

Figure 12-1 Domain Name Access page

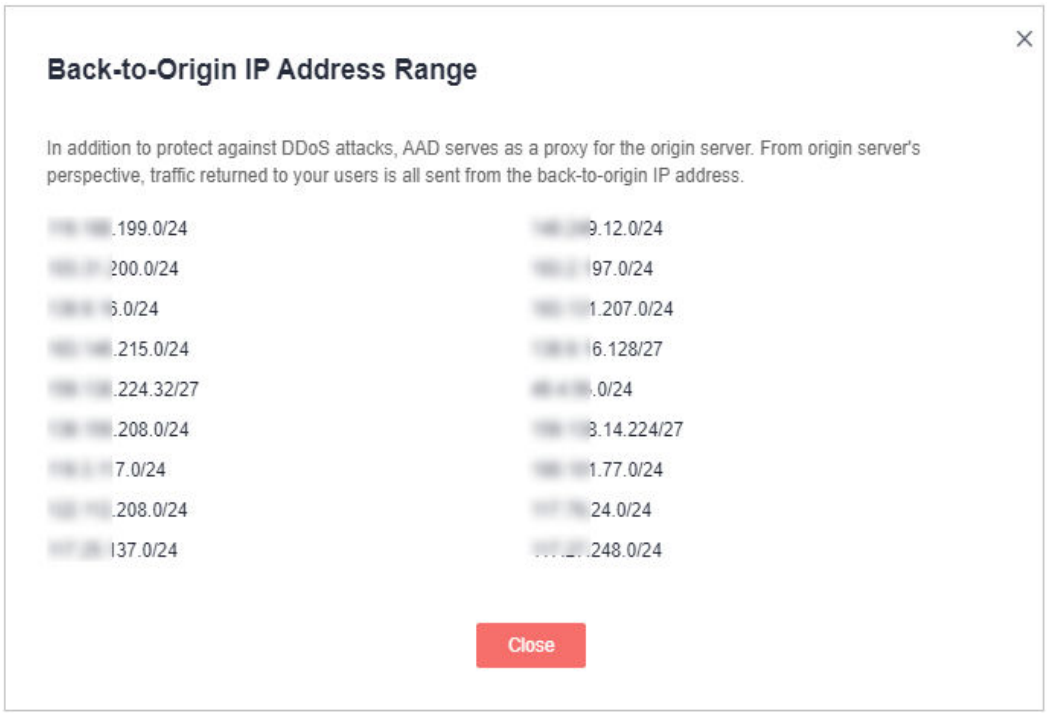


Step 3 On the displayed page, click **Back-to-Origin IP Address Range**.

 Copyright © Huawei Technologies Co., Ltd.

Step 4 In the displayed **Back-to-Origin IP Address Range** dialog box, view the back-to-origin IP address range and then whitelist the IP addresses to the firewall or other protective software on the origin server.

Figure 12-2 Back-to-Origin IP Address Range



----End

 Copyright © Huawei Technologies Co., Ltd.

13 Viewing a Protection Report

Scenarios

AAD shows normal traffic and attack traffic in two dimensions: byte and packet. You can view the normal traffic and attack traffic to know your network security situation.

This section describes how to view an AAD report.

Precautions

You can view the attack protection details (latest 90 days) of all AAD instances and all protected domain names on the AAD console.

Prerequisites

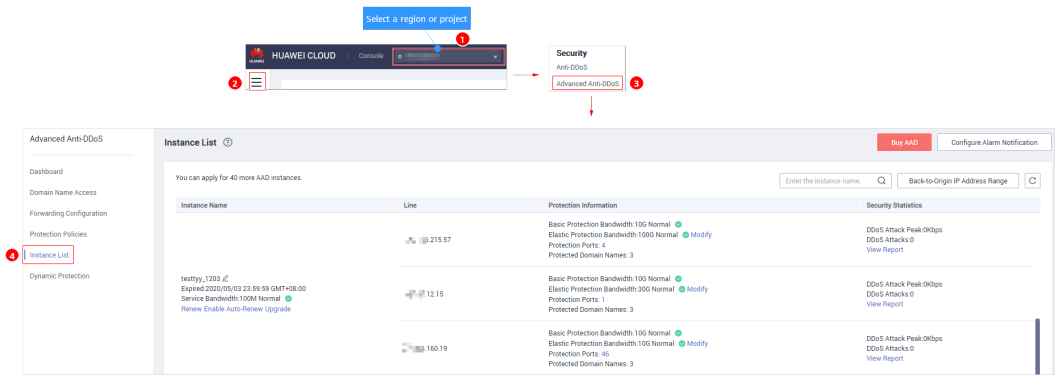
The services have been connected to AAD.

Procedure

Step 1 **Log in to the management console.**

Step 2 Follow the procedure in the following figure to enter the **Advanced Anti-DDoS** console page. In the navigation pane on the left, choose **Instance List**.

Figure 13-1 Instance list entry



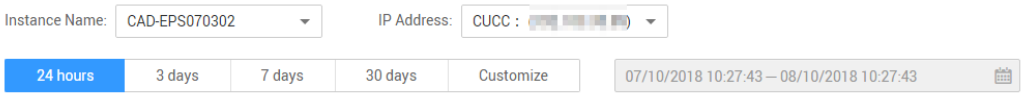
 Copyright © Huawei Technologies Co., Ltd.

Step 3 Select an instance and click **View Report** in the **Security Statistics** column.

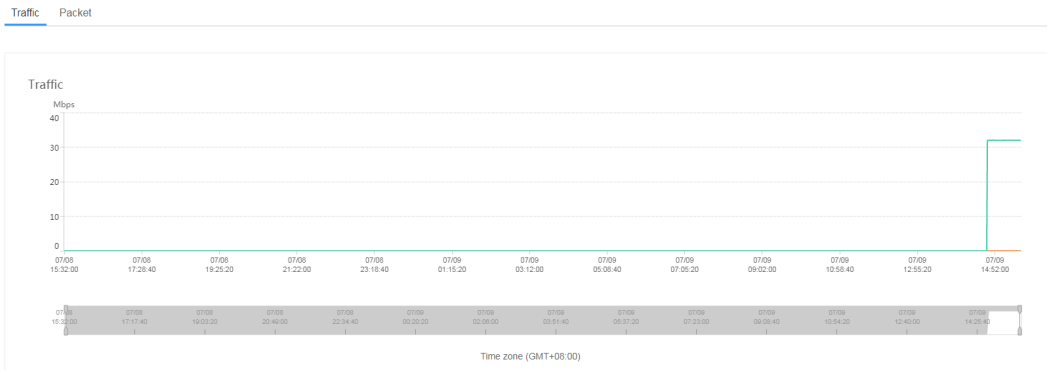
Step 4 Select the instance and IP address for which you want to view the protection report. Set the time range for the report, which includes the following options:

- **24 hours**: provides historical protection data of the last 24 hours. The minimum scale of the timeline is 10 seconds.
- **3 days**: provides historical protection data of the last 3 days. The minimum scale of the timeline is 5 minutes.
- **7 days**: provides historical protection data of the last 7 days. The minimum scale of the time axis is 1 hour.
- **30 days**: provides historical protection data of the last 30 days. The minimum scale of the time axis is 1 hour.
- Customize: Click , select the start date and time and end date and time, and click **OK**.

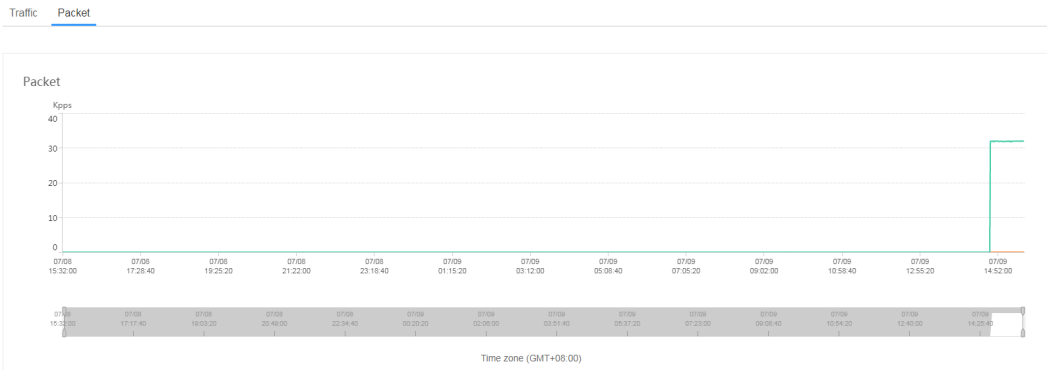
  You can query historical protection data of the last 90 days. The minimum scale of the timeline is determined based on the time range set and has the following options:
  - Time range ≤ 24 hours: The minimum scale is 10 seconds.
  - 24 hours < time range ≤ 3 days: The minimum scale is 5 minutes.
  - 3 days < time range ≤ 90 days: The minimum scale is 1 hour.



Step 5 Click the **Traffic** tab to view the traffic report.

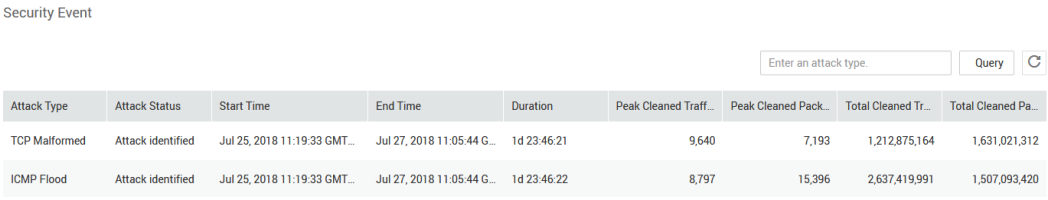


Step 6 Click the **Packet** tab to view the packet report.



 Copyright © Huawei Technologies Co., Ltd.

Step 7 View security events. Security event information can be queried by the attack type.


Security Event

Enter an attack type. Query

Attack Type	Attack Status	Start Time	End Time	Duration	Peak Cleaned Traff...	Peak Cleaned Pack...	Total Cleaned Tr...	Total Cleaned Pa...
TCP Malformed	Attack identified	Jul 25, 2018 11:19:33 GMT...	Jul 27, 2018 11:05:44 G...	1d 23:46:21	9,640	7,193	1,212,875,164	1,631,021,312
ICMP Flood	Attack identified	Jul 25, 2018 11:19:33 GMT...	Jul 27, 2018 11:05:44 G...	1d 23:46:22	8,797	15,396	2,637,419,991	1,507,093,420

----End

 Copyright © Huawei Technologies Co., Ltd.

14 (Optional) Managing Enterprise Projects

14.1 Creating an Enterprise Project

Scenarios

The enterprise project feature allows you to create your own projects. For each project, you can separately manage AAD resources. Each project has its own AAD instance bills.

This section provides guidance on the management of enterprise projects for customers with enterprise project management rights.

AAD supports multi-project management, allowing enterprises to manage their AAD resources by project.

Prerequisites

You have obtained the username and password for logging in to the management console and managing enterprise projects.

Procedure

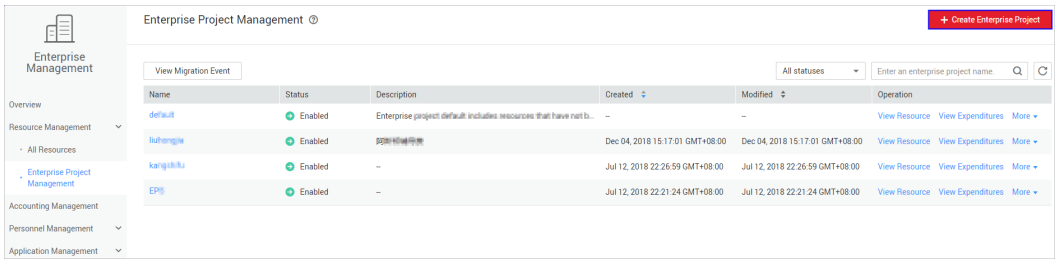
Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, click **Enterprise**. The **Enterprise Management** console is displayed.

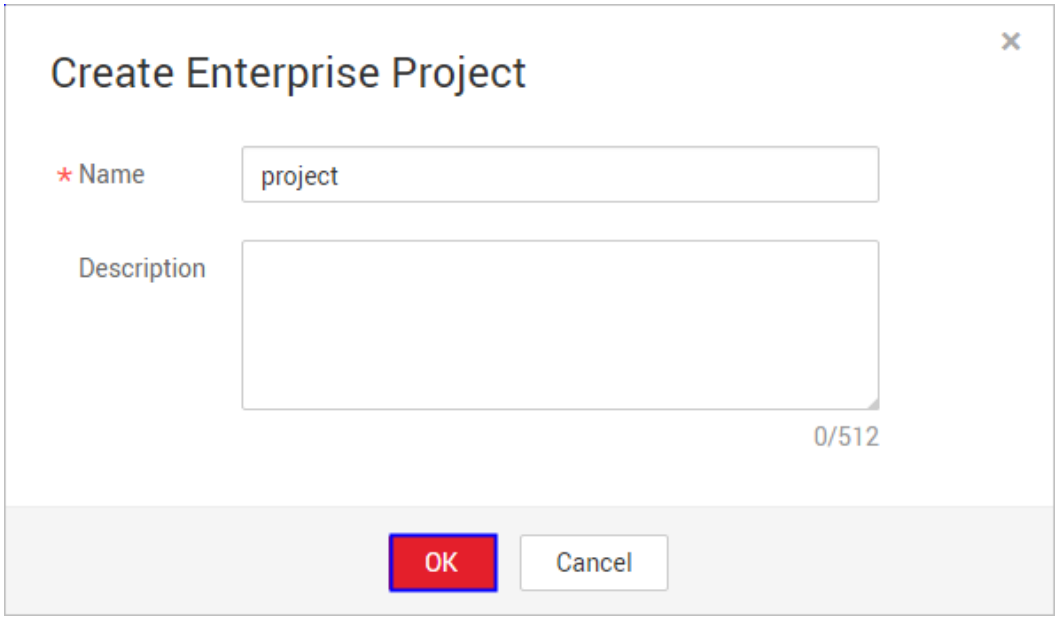


Step 3 In the navigation pane on the left, choose **Enterprise Project Management**. In the right pane, click **Create Enterprise Project**.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 In the **Create Enterprise Project** dialog box, enter the project name and description, and click **OK**.



----End

14.2 Disabling an Enterprise Project

Scenarios

AAD supports multi-project management, allowing enterprises to manage their AAD resources by project.

Prerequisites

You have obtained the username and password for logging in to the management console and managing enterprise projects.

Procedure

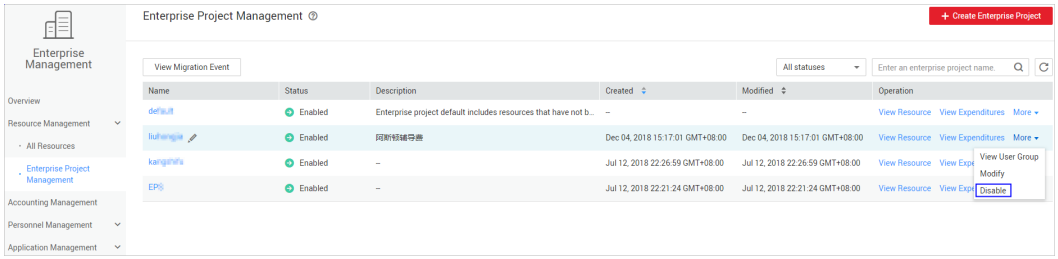
Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, click **Enterprise**. The **Enterprise Management** console is displayed.

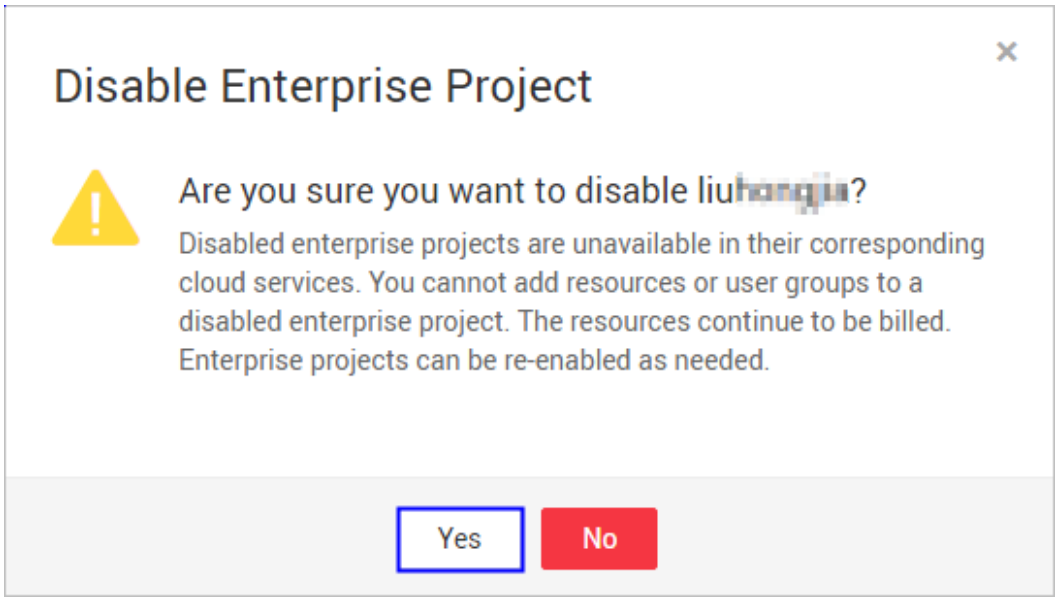


 Copyright © Huawei Technologies Co., Ltd.

Step 3 In the navigation pane on the left, choose **Enterprise Project Management**. In the right pane, locate the target enterprise project, click **More**, and select **Disable** in the **Operation** column.



Step 4 In the **Disable Enterprise Project** dialog box, click **Yes**.



----End

14.3 Managing Enterprise Project Resources

Scenarios

AAD supports enterprise project management, allowing enterprises to manage their AAD resources by enterprise project.

Prerequisites

You have obtained the username and password for logging in to the management console and managing enterprise projects.

Procedure

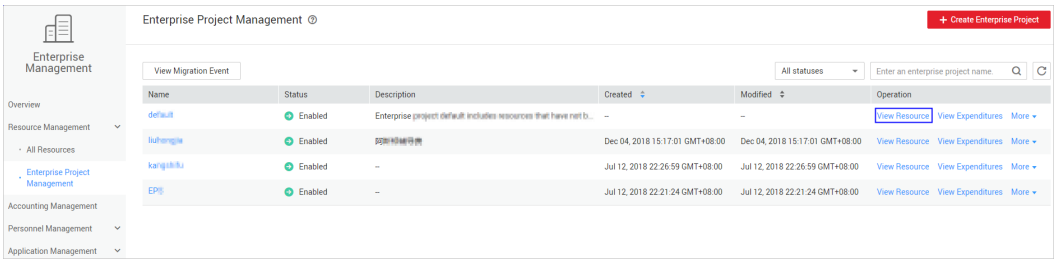
Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, click **Enterprise**. The **Enterprise Management** console is displayed.

 Copyright © Huawei Technologies Co., Ltd.

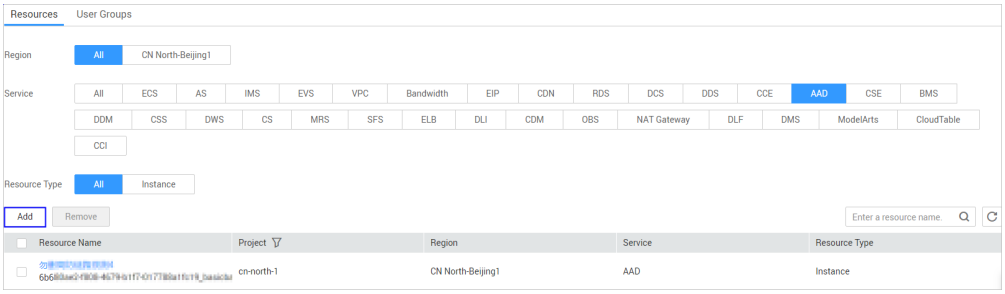


Step 3 In the navigation pane on the left, choose **Resource Management** > **Enterprise Project Management**. In the right pane, locate the target enterprise project and click **View Resource** in the **Operation** column.



Step 4 Add an AAD instance from another enterprise project.

1. On the **Resources** tab, set **Service** to **AAD** and click **Add**.

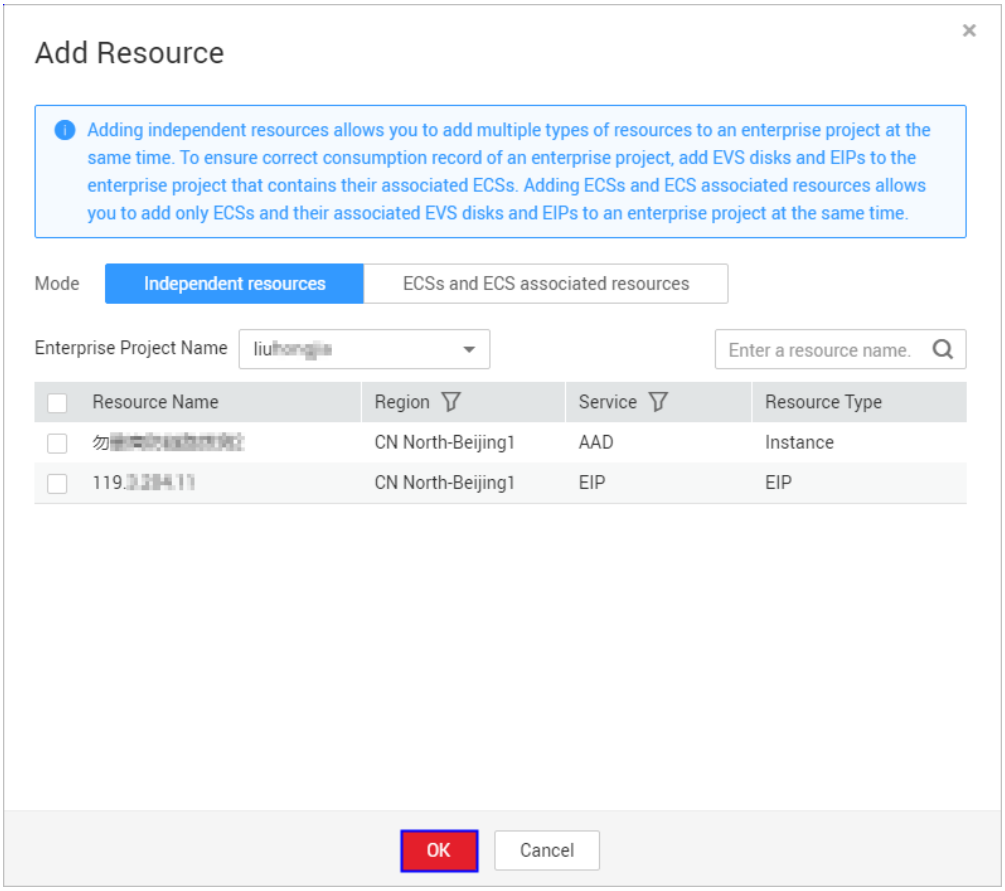


2. In the **Add Resource** dialog box, select the enterprise project name and the AAD instances.

   NOTE

   You cannot change the enterprise project of an AAD instance for which a domain name is added for protection.

 Copyright © Huawei Technologies Co., Ltd.



3. Click **OK**.

Step 5 Remove an AAD instance from the enterprise project.

1. On the **Resources** tab, set **Service** to **AAD**, select the AAD instances to be removed, and click **Remove**.

   NOTE

   You cannot change the enterprise project of an AAD instance for which a domain name is added for protection.

2. In the **Remove Resource** dialog box, select the destination enterprise project to which the AAD instances are to be added and click **OK**.

----End

14.4 Managing a User Group

Scenarios

AAD supports enterprise project management, allowing enterprises to manage their AAD resources by enterprise project.

Prerequisites

You have obtained the username and password for logging in to the management console and managing enterprise projects.

 Copyright © Huawei Technologies Co., Ltd.

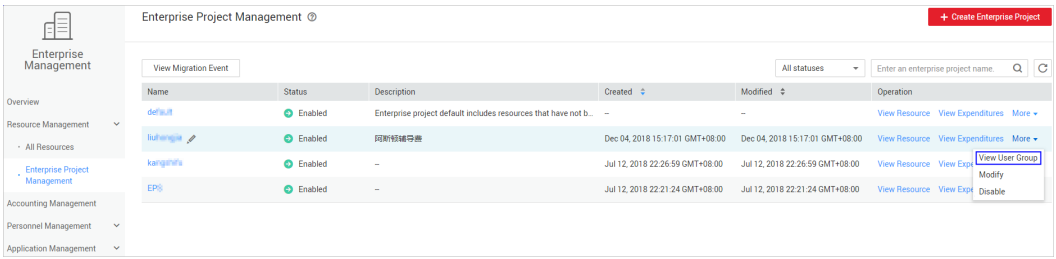
Procedure

Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, click **Enterprise**. The **Enterprise Management** console is displayed.



Step 3 In the navigation pane on the left, choose **Resource Management** > **Enterprise Project Management**. In the right pane, locate the target enterprise project, click **More**, and select **View User Group** in the **Operation** column.

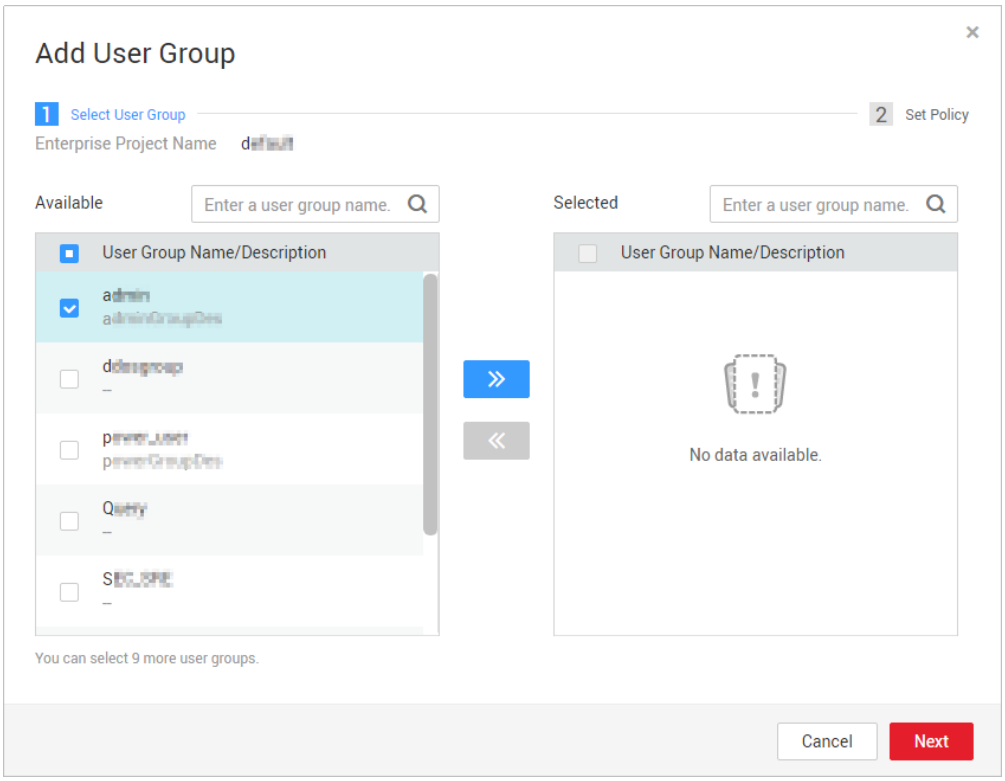


Step 4 Add a user group.

1. Click **Add User Group**.



2. In the **Available** area, select the user groups that you want to add to the enterprise project.



 Copyright © Huawei Technologies Co., Ltd.

3. Click » to move the selected user groups to the **Selected** area.
4. Click **Next**. In the **Available** area, select the policies to be added to the enterprise project.
5. Click » to move the selected policies to the **Selected** area.
6. Click **OK**.

Step 5 Remove a user group.

1. You can remove user groups one by one or in batches.
   - To remove one user group, click **Remove** in the **Operation** column of the user group.
   - To remove user groups in batches, select user groups and click **Remove** above the user group list.
2. In the **Remove User Group** dialog box, click **Yes**.

----End

14.5 Viewing Expenditures of an Enterprise Project

Scenarios

AAD supports enterprise project management, allowing enterprises to manage their AAD resources by enterprise project.

Prerequisites

You have obtained the username and password for logging in to the management console and managing enterprise projects.

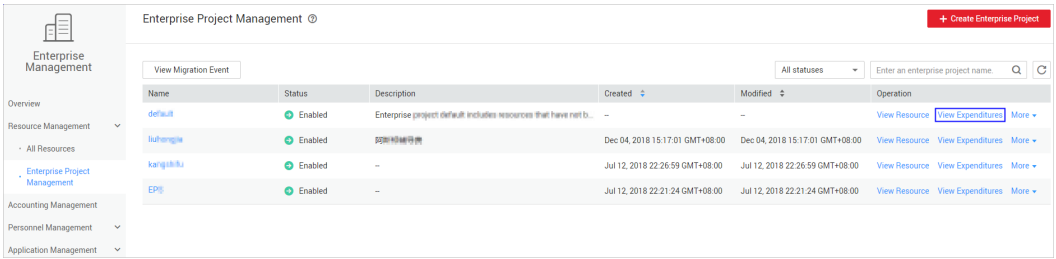
Procedure

Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, click **Enterprise**. The **Enterprise Management** console is displayed.

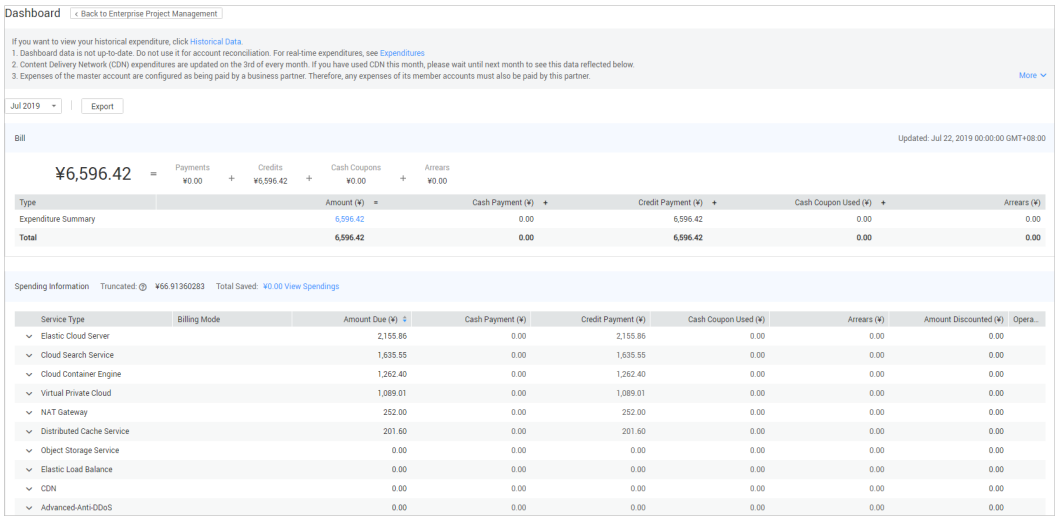


Step 3 In the navigation pane on the left, choose **Resource Management** > **Enterprise Project Management**. In the right pane, locate the target enterprise project and click **View Expenditures** in the **Operation** column.



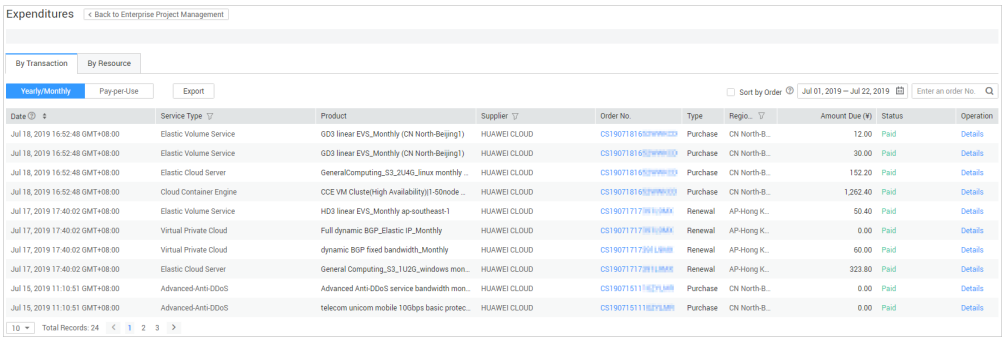
 Copyright © Huawei Technologies Co., Ltd.

Step 4 On the **Dashboard** page, select a month to view the expenditures about the project in that month.



Step 5 To the right of **Spending Information**, click **View Spendings** to view detailed spending information of the project.

- The **By Transaction** page shows expenditure data by transaction, for example, the expenditure details of paying a yearly/monthly subscription at a certain point in time.
- The **By Resource** page shows expenditure data by resource, for example, expenditures of a pay-per-use AAD instance in a certain month.



----End

14.6 Unsubscribing from an Enterprise Project

Scenarios

AAD supports multi-project management, allowing enterprises to manage their AAD resources by project.

Prerequisites

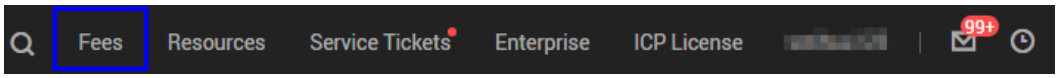
You have obtained the username and password for logging in to the management console and managing enterprise projects.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 In the upper right part of the page, click **Fees**. The **Billing Center** page is displayed.



Step 3 In the navigation pane on the left, click **Unsubscriptions and Changes**.

Step 4 For details about unsubscription, see **Unsubscriptions**.

----End

Copyright © Huawei Technologies Co., Ltd.

15 Permissions Management

15.1 Creating a User and Granting the AAD Access Permission

You can use **Identity and Access Management (IAM)** to implement refined permission control for AAD resources. To be specific, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to AAD resources.
- Grant only the permissions required for users to perform a task.
- Entrust a HUAWEI CLOUD account or cloud service to perform professional and efficient O&M to your AAD resources.

If your HUAWEI CLOUD account does not need individual IAM users for permissions management, then you may skip over this chapter.

This section describes the procedure for granting permissions (see **Figure 15-1**).

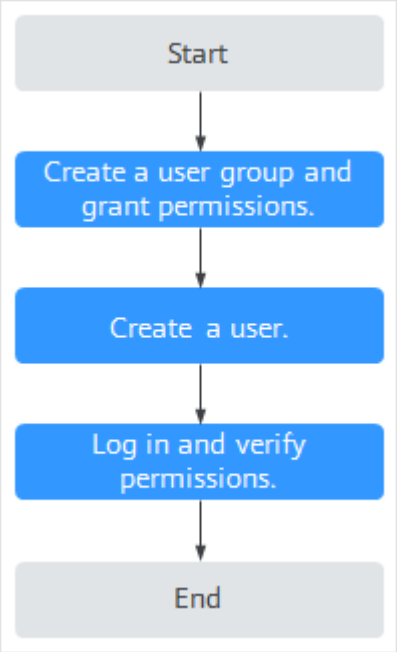
Prerequisites

Before assigning permissions to a user group, you should learn about the AAD permissions that can be added to the user group, and select the permissions based on the site requirements. For details about the permissions, see **Permissions Management**. For the permissions of other services, see section "Permissions Management".

 Copyright © Huawei Technologies Co., Ltd.

Process

Figure 15-1 Process for granting permissions



1. **Creating a User Group and Assigning Permissions**

   Create a user group on the IAM console, and grant the AAD administrator permissions (**CAD Administrator**) to the group.

2. **Creating an IAM User**

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify the permission.

   Log in to the management console by using the user created in **2**, and verify that the user only has read permissions for AAD.

   In **Service List** on the HUAWEI CLOUD console, select any other services (for example, there is only the **CAD Administrator** policy). If a message indicating that the permission is insufficient is displayed, the **CAD administrator** permission takes effect.

 Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2020-11-09	This is the twenty-sixth official release. Updated screenshots and descriptions in **Enabling Alarm Notification**.
2020-10-30	This issue is the twenty-fifth official release. Deleted the description of dynamic protection groups.
2020-10-09	This issue is the twenty-fourth official release. • Added **Viewing Protection Details**. • Deleted section "Overview".
2020-09-21	This issue is the twenty-third official release. • Deleted the descriptions of new BGP in **Purchasing AAD Instances**. • Deleted the descriptions of new BGP in **Line Packages**.
2020-09-07	This issue is the twenty-second official release. Optimized descriptions in **Upgrading Specifications**.
2020-06-29	This issue is the twenty-first official release. • Added the description of new BGP in **Purchasing AAD Instances**. • Added the description of new BGP in **Line Packages**.
2020-06-15	This issue is the twentieth official release. Added **Updating a Certificate**.

 Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2020-06-09	This issue is the nineteenth official release. • Updated the screenshots in **Viewing a Back-to-Origin IP Address Range**. • Added permission restrictions in **Purchasing AAD Instances**.
2020-04-08	This issue is the eighteenth official release. Updated some screenshots.
2020-03-12	This issue is the seventeenth official release. Modified links in **Creating a User and Granting the AAD Access Permission**.
2020-01-20	This issue is the sixteenth official release. • Optimized descriptions in **Creating a User and Granting the AAD Access Permission**. • Optimized descriptions in **Connecting a Website Service to AAD**.
2020-01-07	This issue is the fifteenth official release. • Added **Creating a User and Granting the AAD Access Permission**. • Added section "Enabling Advanced Anti-DDoS".
2019-06-28	This issue is the fourteenth official release. Added section "Permissions Management".
2019-04-17	This issue is the thirteenth official release. • Added **Configuring a Blacklist and a Whitelist**. • Added **Configuring Traffic Control**.
2018-08-13	This issue is the twelfth official release. Updated screenshots of all instances in **Changing the Name of an AAD Instance**.
2018-08-02	This issue is the eleventh official release. Added descriptions about adding, deleting, and exporting forwarding rules in batches in **Configuring a Forwarding Rule**.
2018-07-12	This issue is the tenth official release. • Added section "Managing Enterprise Projects". • Added **Modifying Resolution Lines for High-Defense IP Addresses of a Domain Name**.

Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2018-07-04	This issue is the ninth official release. Deleted ports **80**, **8080**, **8081**, **443**, **7443**, and **8443** from **Configuring a Forwarding Rule**.
2018-06-07	This issue is the eighth official release. • Added **Connecting a Website Service to AAD**. • Added **Connecting a Non-website Service to AAD**. • Added **Modifying Domain Name Configuration**. • Deleted section "(Optional) Accessing a Protected Domain Name".
2018-05-08	This issue is the seventh official release. Added ports **8080**, **8081**, **443**, **7443**, and **8443** in **Configuring a Forwarding Rule**.
2018-01-24	This issue is the sixth official release. • Added two lines: CUCC and BGP. • Added a region: East China 2.
2017-12-28	This issue is the fifth official release. Modified screenshots and descriptions in **Viewing a Back-to-Origin IP Address Range**.
2017-12-21	This issue is the fourth official release. Added section "Managing a Domain Name".
2017-11-03	This issue is the third official release. • Added **Viewing a Back-to-Origin IP Address Range**. • Added the description for the number of modification times in **Changing the Elastic Protection Bandwidth**.
2017-10-28	This issue is the second official release. Changed the number of AAD instances to purchase.
2017-09-14	This issue is the first official release.

Copyright © Huawei Technologies Co., Ltd.