Anti-DDoS

Best Practices

Issue	04
Date	2021-08-06

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Configuring Alarm Notifications

Scenario

An alarm notification will be sent to the endpoint you have configured if a DDoS attack is detected after you enable the alarm notification.

Prerequisites

- You have enabled Simple Message Notification (SMN).
- You have purchased at least one public IP address.

Constraints

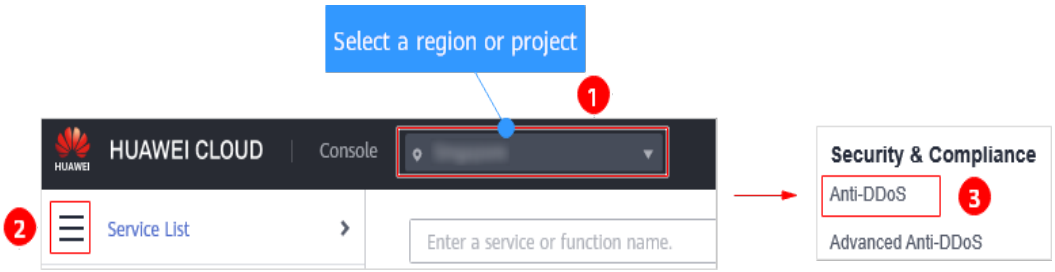
- Simple Message Notification (SMN) is a paid service. For details, see **Product Pricing Details**.
- Before enabling alarm notification, **create a topic** and **add a subscription to the topic** in SMN.

Procedure

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

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Anti-DDoS**.

Figure 1-1 Anti-DDoS



Step 3 On the **Anti-DDoS** page, click the **Alarm Notifications** tab and configure alarm notification. For details about the parameter setting, see **Figure 1-2**.

Figure 1-2 Configure alarm notifications

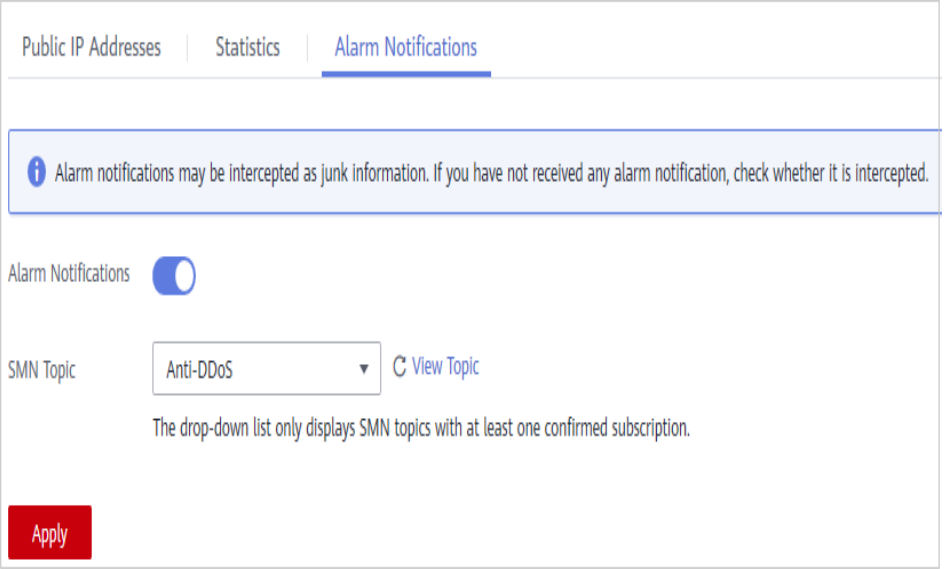


Table 1-1 Parameters required for configuring alarm notifications

Parameter	Description	Example Value
Alarm Notifications	Indicates whether to enable the alarm notification. The options are as follows: • : enabled • : disabled If the function is disabled, click to set it to .	
SMN Topic	You can select an existing topic or click **View Topic** to create a topic.	-

Click **View Topic** to switch to the SMN console where you can create a topic and configure the endpoint to receive the alarm notifications. To create a topic, perform the following steps:

1. Follow the instructions described in **Creating a Topic** to create a topic.
2. Follow the instructions described in **Adding a Subscription** to configure an endpoint, such as mobile number or email address, to receive the alarm notifications.

For more information about topics and subscriptions, see **Simple Message Notification**.

Step 4 Click **Apply** to enable alarm notification.

----End

2 Connecting to a Server Routed to a Black Hole

Scenario

When your server is under a traffic flooding attack, a black hole will be triggered to block all accesses from the Internet. You can connect to a server which a black hole has been triggered for through an ECS.

Prerequisites

- You have purchased at least one public IP address.
- The username and password for logging in to an ECS have been obtained.
- The username and password for logging in to a server which a black hole has been triggered for have been obtained.

Constraints

Ensure the ECS can be accessed and in the same region as the server.

Procedure

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

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click and choose **Computing** > **Elastic Cloud Server**.

Step 4 Log in to the ECS that can be accessed and in the same region as the server which a black hole has been triggered for.

Select a login method and log in to the ECS.

- For details about how to log in to a Windows ECS, see **Windows ECS Login Overview**.
- For details about how to log in to a Linux ECS, see **Linux ECS Login Overview**.

Step 5 Table 2-1 describes how to connect to a server which a black hole has been triggered for.

Table 2-1 Server connection

ECS OS	Blackholed Server OS	Connection Method
Windows	Windows	Use MSTSC to log in to the server which a black hole has been triggered for. 1. Search for **mstsc** in the ECS and click it to open the **Remote Desktop Connection** dialog box. 2. Click **Show Options** in the displayed dialog box. 3. Enter the EIP and username (**Administrator** by default) of the server which a black hole has been triggered for. 4. Click **OK** and enter the login password as prompted to log in to the server.
	Linux	Use a remote login tool, such as PuTTY or Xshell, to log in to the server.
Linux	Windows	1. Install a remote connection tool, such as **rdesktop**. 2. Run the following command to log in to the server which a black hole has been triggered for. **rdesktop -u** *Username* **-p** *Password* **-g** *Resolution EIP bound to the server which a black hole has been triggered for*
	Linux	Run the following command to log in to the server which a black hole has been triggered for. **ssh** *EIP bound to the server which a black hole has been triggered for*

----End

Follow-up Operation

Once you have connected your ECS to a server in the black hole state, you can transfer files to the server and can make whatever configuration changes are necessary.

3 Enhancing DDoS Mitigation Capabilities

Anti-DDoS provides a 500 Mbit/s mitigation capacity against DDoS attacks for free. Attack traffic that exceeds 500 Mbit/s will be routed to a black hole and legitimate traffic will be discarded.

To resume services quickly, it is a better choice to purchase HUAWEI CLOUD Advanced Anti-DDoS to expand protection capabilities.

A Change History

Released On	Description
2021-08-06	This is the fourth official release. Modified the description of the entry on the management console.
2021-06-18	This is the third official release. ● Optimized descriptions in **Configuring Alarm Notifications**. ● Optimized descriptions in **Connecting to a Server Routed to a Black Hole**.
2020-04-08	This is the second official release. Updated some screenshots.
2019-06-21	This is the first official release.

