Host Security Service

User Guide

Issue	34
Date	2022-05-26

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

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

Trademarks and Permissions

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

Notice

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

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

Contents

 Copyright © Huawei Technologies Co., Ltd.

1 Enabling HSS

1.1 Step 1: Purchase HSS Quota

Purchase HSS for your servers. The premium edition is provided for free if you have purchased the WTP edition.

Recommended Editions

HSS comes in basic, enterprise, premium, and WTP editions. **Table 1-1** describes their application scenarios. For more information, see **Editions**.

NOTICE

- You are advised to deploy HSS on all your servers so that if a virus infects one of them, it will not be able to spread to others and damage your entire network.
- In the pay-per-use mode, HSS stops charging if the servers it protects are stopped.

 Copyright © Huawei Technologies Co., Ltd.

Table 1-1 Recommended editions

Edition	Billing Mode	Scenario
Basic	• Pay-per-use You can use the basic edition for each of your servers for 30 calendar days free or charge. When purchasing an ECS, you can enable the HSS basic edition for free. The free trial lasts 30 days. • Yearly/Monthly The basic edition in yearly/monthly mode does not have a free trial period.	This edition can protect any number of servers, but only part of the security scan capabilities are available. This edition does not provide protection capabilities, nor does it provide support for DJCP MLPS certification. You can use this edition to protect test servers or individual users' servers. The basic edition only provides part of the baseline check and intrusion detection functions, and displays the security risk overview of assets on the cloud. **NOTE** • If the basic edition in yearly/monthly mode expires, HSS resources protecting your servers will be released. • If you select **Yearly/Monthly** and a message indicating insufficient quota is displayed, you need to purchase HSS and then enable it.
Enterprise edition	• Pay-per-use • Yearly/Monthly	Help servers meet basic security compliance requirements (such as virus and Trojan scan, one-click vulnerability fixing, and intrusion detection).

Copyright © Huawei Technologies Co., Ltd.

Edition	Billing Mode	Scenario
Premium	Yearly/ Monthly	For servers that need to meet high security requirements (for example, to protect websites or critical services), the premium or WTP edition is recommended. You are advised to enable the premium or WTP edition for servers that process critical services or are exposed to high risks, for example, servers that expose EIPs, application servers that store important data, and database servers.
Web Tamper Protection	Yearly/ Monthly	For servers that need to protect websites and applications from tampering, the WTP edition is recommended. The premium edition is available for free if you have purchased the WTP edition.

Constraints

- A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- HSS cannot protect **Huawei Cloud** servers across regions. If the servers and HSS quota are in different regions, unsubscribe from the quota and purchase HSS in the region where the server is deployed.
- To protect HUAWEI CLOUD servers, non-HUAWEI CLOUD servers can access only the **CN-Hong Kong** region. You need to purchase protection quotas in this region and use the installation packages or installation command in this region to install the agent on non-HUAWEI CLOUD servers.

Purchasing HSS (for Huawei Cloud Servers)

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the upper right corner of the **Dashboard** page, click **Buy HSS**.

Step 4 On the **Buy HSS** page, set the quota specifications.

1. Select **Yearly/Monthly** for **Billing Mode**.

   HSS can be billed in yearly/monthly or pay-per-use mode.

   NOTE

   - If you select **Pay-per-use**, you do not need to purchase HSS quota. Click **Enable Now** in the lower right corner and enable HSS in the server list.
   - In the **Operation** column of a server, click **Enable**. Set **Billing Mode** to **On-demand**. Set **HSS Edition** to **Basic** or **Enterprise**.

2. Select a region.

   HSS cannot be used across regions. If you purchased a quota in a wrong region, unsubscribe from it and purchase a quota in the region of your servers.

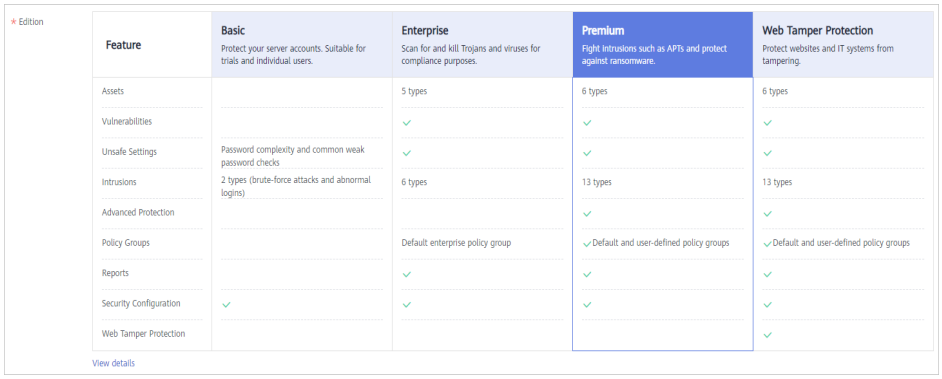
3. Select an edition.

   Select **Basic**, **Enterprise**, **Premium**, or **Web Tamper Protection**. For details about the differences between editions, see **Editions**.

   – If you purchased the basic, enterprise, or premium edition, enable it on the **Servers** page of the HSS console.

   – If you purchased the WTP edition, enable it on the **Server Protection** page of the WTP console.

   Figure 1-1 Editions

   * Edition

Feature	Basic Protect your server accounts. Suitable for trials and individual users.	Enterprise Scan for and kill Trojans and viruses for compliance purposes.	Premium Fight intrusions such as APTs and protect against ransomware.	Web Tamper Protection Protect websites and IT systems from tampering.
Assets		5 types	6 types	6 types
Vulnerabilities		✓	✓	✓
Unsafe Settings	Password complexity and common weak password checks	✓	✓	✓
Intrusions	2 types (brute-force attacks and abnormal logins)	6 types	13 types	13 types
Advanced Protection			✓	✓
Policy Groups		Default enterprise policy group	✓ Default and user-defined policy groups	✓ Default and user-defined policy groups
Reports		✓	✓	✓
Security Configuration	✓	✓	✓	✓
Web Tamper Protection				✓

   View details

4. Select an enterprise project.

   Select an enterprise project from the drop-down list.

   Selections are available only if you logged in using an enterprise account, or if you have enabled the enterprise project function. You can contact your service manager to enable this function and put cloud resources and members under enterprise projects for centralized management.

   NOTE

   – Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.

5. Select the amount of time you want to use HSS for.

   You are advised to select **Auto-renew** to ensure your servers are always protected.

   If you select **Auto-renew**, the system will automatically renew your subscription as long as your account balance is sufficient. The renewal period is the same as the required duration.

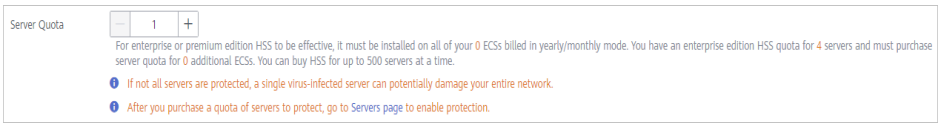
   If you do not select **Auto-renew**, manually renew the service before it expires.

6. Set the number of protected servers.

   You cannot modify the quota of an edition after its purchase is complete. You can unsubscribe from it and purchase again. There is no quota limit.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 Protected servers (enterprise edition)



NOTE

If you have enabled the enterprise project function, you only need to purchase quotas for the servers in your enterprise project.

Step 5 In the lower right corner of the page, click **Next**.

For details about pricing, see **Product Pricing Details**.

Step 6 After confirming that the order, select **I have read and agree to the Host Security Service Disclaimer** and click **Pay Now**.

Step 7 Click **Pay** and complete the payment.

----End

Purchasing HSS (for Non-HUAWEI CLOUD Servers)

Non-HUAWEI CLOUD servers can access only the **CN-Hong Kong** region. You need to purchase protection quotas in this region and use the installation packages or installation command in this region to install the agent on non-HUAWEI CLOUD servers.

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the upper right corner of the **Dashboard** page, click **Buy HSS**.

Step 4 On the **Buy HSS** page, set the quota specifications.

1. Select **Yearly/Monthly** for **Billing Mode**.

   HSS can be billed in yearly/monthly or pay-per-use mode.

   NOTE

   - If you select **Pay-per-use**, you do not need to purchase HSS quota. Click **Enable Now** in the lower right corner and enable HSS in the server list.
   - In the **Operation** column of a server, click **Enable**. Set **Billing Mode** to **On-demand**. Set **HSS Edition** to **Basic** or **Enterprise**.

2. Select a region.

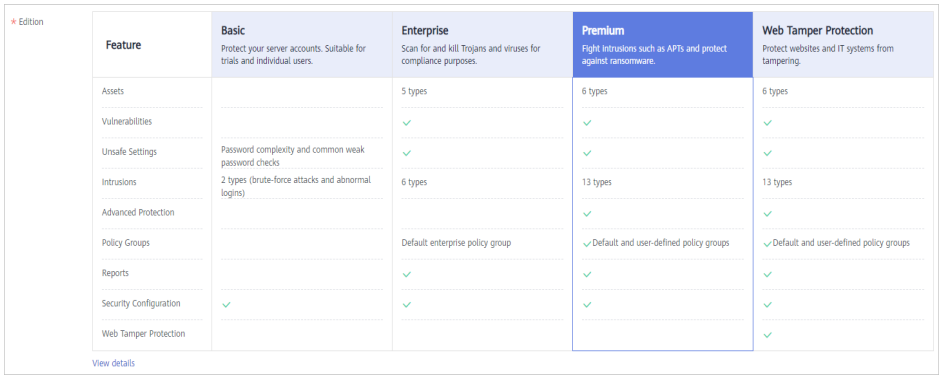
   Non-HUAWEI CLOUD servers can access only the **CN-Hong Kong** region. You need to purchase protection quotas in this region and use the installation packages or installation command in this region to install the agent on non-HUAWEI CLOUD servers.

3. Select an edition.

   Select **Basic**, **Enterprise**, **Premium**, or **Web Tamper Protection**. For details about the differences between editions, see **Editions**.

- If you purchased the basic, enterprise, or premium edition, enable it on the **Servers** page of the HSS console.
- If you purchased the WTP edition, enable it on the **Server Protection** page of the WTP console.

Figure 1-3 Editions



* Edition	Basic	Enterprise	Premium	Web Tamper Protection
Feature	Protect your server accounts. Suitable for trials and individual users.	Scan for and kill Trojans and viruses for compliance purposes.	Fight intrusions such as APTs and protect against ransomware.	Protect websites and IT systems from tampering.
Assets		5 types	6 types	6 types
Vulnerabilities		✓	✓	✓
Unsafe Settings	Password complexity and common weak password checks	✓	✓	✓
Intrusions	2 types (brute-force attacks and abnormal logins)	6 types	13 types	13 types
Advanced Protection			✓	✓
Policy Groups		Default enterprise policy group	✓ Default and user-defined policy groups	✓ Default and user-defined policy groups
Reports		✓	✓	✓
Security Configuration	✓	✓	✓	✓
Web Tamper Protection				✓

View details

4. Select an enterprise project.

   Select an enterprise project from the drop-down list.

   Selections are available only if you logged in using an enterprise account, or if you have enabled the enterprise project function. You can contact your service manager to enable this function and put cloud resources and members under enterprise projects for centralized management.

   NOTE

   - Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.

5. Select the amount of time you want to use HSS for.

   You are advised to select **Auto-renew** to ensure your servers are always protected.

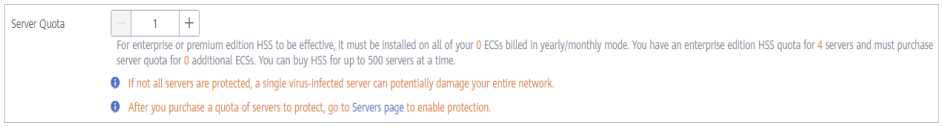
   If you select **Auto-renew**, the system will automatically renew your subscription as long as your account balance is sufficient. The renewal period is the same as the required duration.

   If you do not select **Auto-renew**, manually renew the service before it expires.

6. Set the number of protected servers.

   You cannot modify the quota of an edition after its purchase is complete. You can unsubscribe from it and purchase again. There is no quota limit.

Figure 1-4 Protected servers (enterprise edition)



Server Quota: 1

For enterprise or premium edition HSS to be effective, it must be installed on all of your 0 ECSs billed in yearly/monthly mode. You have an enterprise edition HSS quota for 4 servers and must purchase server quota for 0 additional ECSs. You can buy HSS for up to 500 servers at a time.

If not all servers are protected, a single virus-infected server can potentially damage your entire network.

After you purchase a quota of servers to protect, go to Servers page to enable protection.

NOTE

If you have enabled the enterprise project function, you only need to purchase quotas for the servers in your enterprise project.

Copyright © Huawei Technologies Co., Ltd.

Step 5 In the lower right corner of the page, click **Next**.

For details about pricing, see **Product Pricing Details**.

Step 6 After confirming that the order, select **I have read and agree to the Host Security Service Disclaimer** and click **Pay Now**.

----End

Verification

After you pay for your order, check the purchased HSS edition, quota status, and protected servers on the **Quota** tab of the **Servers** page.

Follow-Up Procedure

Unsubscription

If you purchased HSS in the wrong edition or region, you can first unsubscribe from it and then purchase the correct quota.

Switching editions

If the current edition does not meet your service requirements, you can purchase HSS in your desired edition and switch to this edition. For details, see **(Optional) Step 5: Switching the HSS Edition**.

1.2 Step 2: Install an Agent

1.2.1 Installing an Agent on the Linux OS

You can enable HSS only after the HSS agent is installed on your servers. This topic describes how to install the agent on a server running a Linux OS. For details about installation on the Windows OS, see **Installing an Agent on the Windows OS**.

NOTE

WTP and HSS can use the same agent on a server.

The agent status will be refreshed 5 to 10 minutes after it is installed. You are advised to restart the server before enabling HSS.

Prerequisites

- An EIP has been bound to the offline server where the agent is to be installed.
- The online server where the agent is to be installed must be able to communicate with the network segment. The security group of your server must allow outbound access to port 443 on the 100.125.0.0/16 network segment.
- A remote management tool, such as Xftp, SecureFX, and WinSCP, has been installed on your PC.
- The Security-Enhanced Linux (SELinux) firewall has been disabled. The firewall affects agent installation and should remain disabled until the agent is installed.

 Copyright © Huawei Technologies Co., Ltd.

Constraints

- **Huawei Cloud servers**

  Ensure you have purchased HSS in your server region and have used the installation package or installation command in the region to install HSS agents on your servers. If the server and HSS quota are in different regions, unsubscribe from the quota and purchase a quota in the region where the server is deployed.

- **Non-Huawei Cloud servers**
  - So far, HSS can be installed on non-HUAWEI CLOUD servers only in the **CN-Hong Kong** region.
  - For non-Huawei Cloud servers to access HSS, the servers need to access Huawei Cloud first. After the agent is installed on a server, the server will be displayed on the console. You can find it by searching for its IP address.

NOTICE

- For better compatibility and service experience, you are advised to use Huawei Cloud servers.
- If a piece of third-party security software, such as McAfee, has been installed on your server, stop the software and clear its configuration before installing an HSS agent to avoid installation failures.

Impact on the System

The HSS agent does not affect server running. The agent runs scan tasks to scan all servers, monitors server security, and reports collected server information to the cloud protection center. Servers without the agent cannot be protected by HSS. The console does not display system vulnerabilities, baseline risks, intrusion events, or security reports on these servers.

Default Installation Path

The agent installation path on servers running the Linux OS cannot be customized. The default path is:

/usr/local/hostguard/

Installing an Agent Using Commands

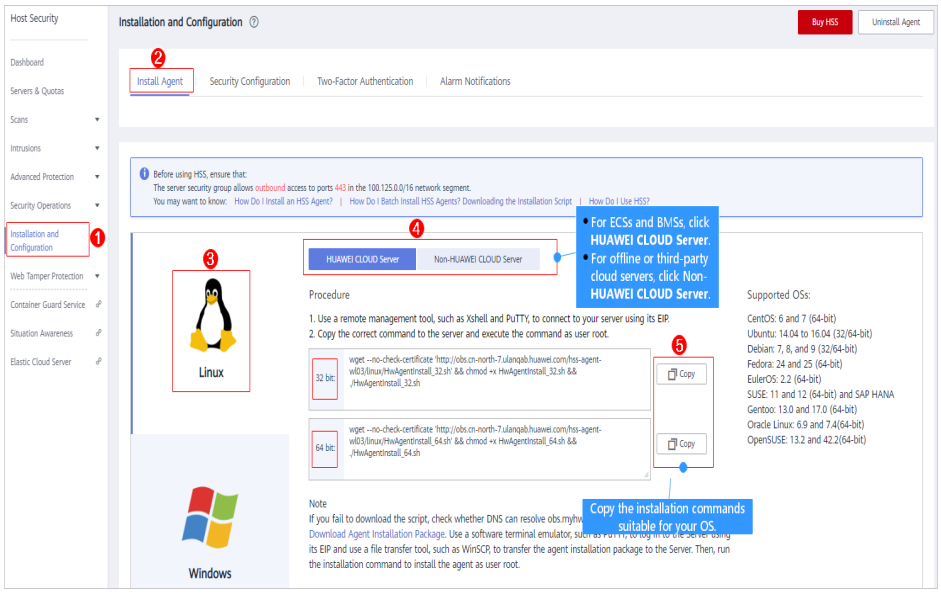
This procedure involves logging in to the server and running commands. It takes 3 to 5 minutes for the console to update the agent status after agent installation.

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Installation and Configuration**. On the **Install Agent** tab, copy the required installation command.

Figure 1-5 Copying the command for installing the agent



Step 4 Remotely log in to the server where the agent is to be installed.

- HUAWEI CLOUD server
  - Log in to the ECS console, locate the target server, and click **Remote Login** in the **Operation** column to log in to the server. For details, see **Login Using VNC**.
  - If your server has an EIP bound, you can also use a remote management tool, such as Xftp, SecureFX, or WinSCP, to log in to the server and install the agent on the server as user **root**.
- Non-HUAWEI CLOUD server

  Use Xftp, SecureFX, or WinSCP to log in to the server for installing the agent as user **root**.

Step 5 Paste the copied installation command and press **Enter** to install the agent on the server.

If information similar to the following is displayed, the agent is successfully installed:

```
Preparing...                ########################### [100%]
1:hostguard                 ########################### [100%]
Hostguard is running.
Hostguard installed.
```

Step 6 Run the **service hostguard status** command to check the running status of the agent.

If the following information is displayed, the agent is running properly:

```
Hostguard is running
```

It takes 3 to 5 minutes for the console to update the agent status after agent installation.

----End

 Copyright © Huawei Technologies Co., Ltd.

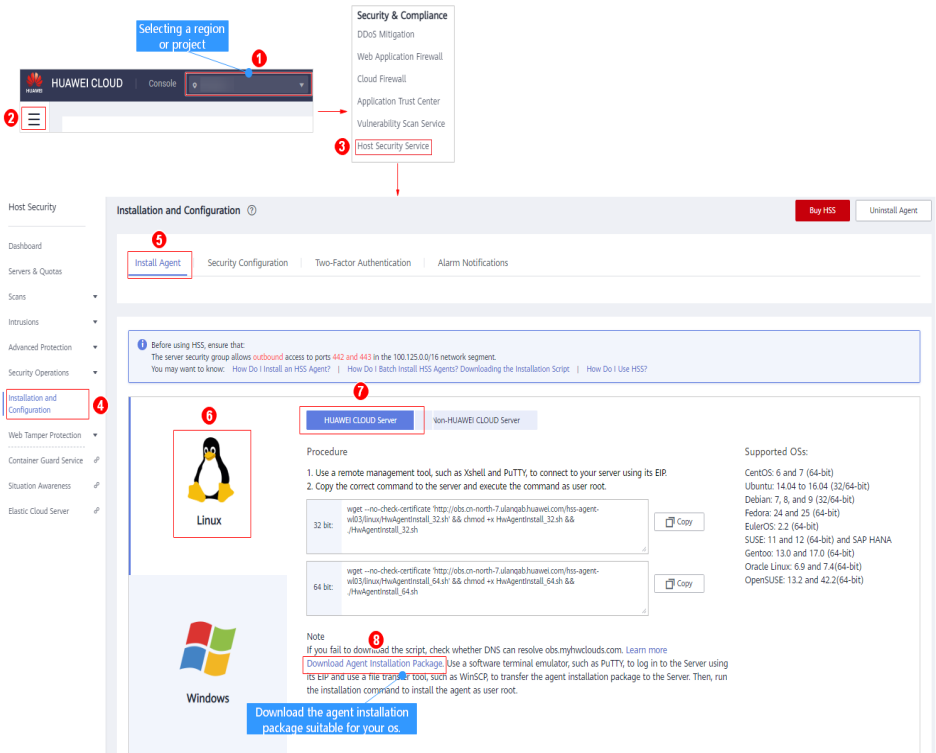
(For Huawei Cloud Servers) Installing an Agent Using an Installation Package

Download the agent installation package, upload it to the server where the agent is to be installed, and run the installation command on the server to install the agent.

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

Step 2 In the navigation pane on the left, choose **Installation and Configuration**. On the **Install Agent** tab, download the agent package.

Figure 1-6 Downloading the agent installation package



Step 3 Download the agent to be installed based on the server OS version.

Step 4 Use a file transfer tool, such as Xftp, SecureFX, or WinSCP, to upload the agent installation package to the server.

Step 5 Remotely log in to the server where the agent is to be installed.

- Log in to the ECS console, locate the target server, and click **Remote Login** in the **Operation** column to log in to the server. For details, see **Login Using VNC**.
- If your server has an EIP bound, you can also use a remote management tool, such as Xftp, SecureFX, or WinSCP, to log in to the server and install the agent on the server as user **root**.

Step 6 Run **cd** *Installation_package_directory* to access the directory.

Step 7 Run the following command to install the agent on the server:

- For an .rpm package, run **rpm -ivh** *Package_name*.

  NOTE

  To forcibly install the agent, run the **rpm -ivh --force** *Package_name* command.

- For a .deb package, run **dpkg -i** *Package_name*.

  If information similar to the following is displayed, the agent is successfully installed:

```
Preparing...                ########################### [100%]
1:hostguard                  ########################### [100%]
Hostguard is running.
Hostguard installed.
```

Step 8 Run the **service hostguard status** command to check the running status of the agent.

If the following information is displayed, the service is running properly:

```
Hostguard is running
```

It takes 3 to 5 minutes for the console to update the agent status after agent installation.

----End

Follow-Up Procedure

- For details about the agent status and troubleshooting, see **What Should I Do When the Agent Running Status Is Abnormal?**
- For details about handling agent installation failures, see **What Should I Do If Agent Installation Failed?**
- For details about agent uninstallation, see **How Do I Uninstall the Agent?**

1.2.2 Installing an Agent on the Windows OS

You can enable HSS only after an HSS agent is installed on the servers. This topic describes how to install the agent on a server running a Windows OS. For details about how to install an agent on the Linux OS, see **Installing an Agent on the Linux OS**.

NOTE

WTP and HSS can use the same agent on a server.

The agent status will be refreshed 5 to 10 minutes after it is installed. You are advised to restart the server before enabling HSS.

Prerequisites

- An EIP has been bound to the offline server where the agent is to be installed.
- The online server where the agent is to be installed must be able to communicate with the network segment. The security group of your server must allow outbound access to ports 442 and 443 on the 100.125.0.0/16 network segment.
- A remote management tool, such as pcAnywhere and UltraVNC, has been installed on your PC.

Constraints

- **Huawei Cloud servers**

  Ensure you have purchased HSS in your server region and have used the installation package or installation command in the region to install HSS agents on your servers. If the server and HSS quota are in different regions, unsubscribe from the quota and purchase a quota in the region where the server is deployed.

- **Non-Huawei Cloud servers**
  - So far, HSS can be installed on non-HUAWEI CLOUD servers only in the **CN-Hong Kong** region.
  - For non-Huawei Cloud servers to access HSS, the servers need to access Huawei Cloud first. After the agent is installed on a server, the server will be displayed on the console. You can find it by searching for its IP address.

NOTICE

- For better compatibility and service experience, you are advised to use Huawei Cloud servers.
- If a piece of third-party security software, such as McAfee, has been installed on your server, stop the software and clear its configuration before installing an HSS agent to avoid installation failures.

Impact on the System

The HSS agent does not affect server running. The agent runs scan tasks to scan all servers, monitors server security, and reports collected server information to the cloud protection center. Servers without the agent cannot be protected by HSS. The console does not display system vulnerabilities, baseline risks, intrusion events, or security reports on these servers.

Default Installation Path

The agent installation path on servers running the Windows OS cannot be customized. The default path is:

C:\Program Files (x86)\HostGuard

Procedure

There are two ways to install an agent. The procedure describes the second one in detail.

- Method 1: Copy the agent download link. Remotely log in to a server and open the link in Internet Explorer, and download and decompress the agent installation package. Run the agent installation program as an administrator.
- Method 2: Download the agent installation package, upload it to a server, and run the installation command on the server to install the agent.

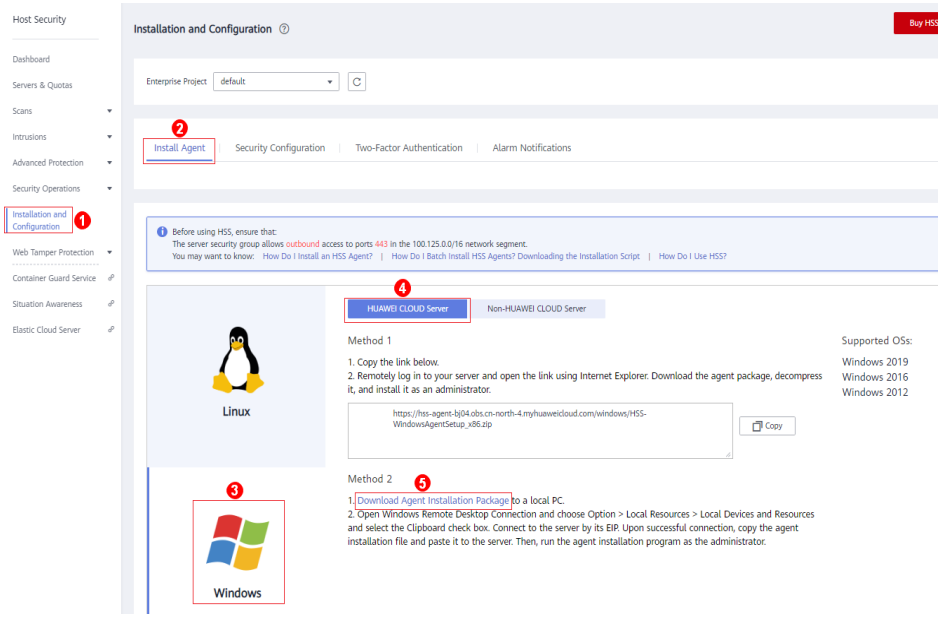
 Copyright © Huawei Technologies Co., Ltd.

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Installation and Configuration**. On the **Install Agent** tab, download the agent package.

Figure 1-7 Installing a Windows agent



Step 4 Remotely log in to the server where the agent is to be installed.

- HUAWEI CLOUD server
  - Log in to the ECS console, locate the target server, and click **Remote Login** in the **Operation** column to log in to the server. For details, see **Login Using VNC**.
  - If an EIP has been bound to the server, you can use Windows Remote Desktop Connection or a third-party remote management tool, such as pcAnywhere and UltraVNC, to log in to the server and install the agent on the server as an administrator.
- Non-HUAWEI CLOUD server

  Log in to the server using Windows Remote Desktop Connection or a third-party remote management tool, such as pcAnywhere and UltraVNC, and install the agent on the server as an administrator.

Step 5 Upload the agent installation package to the server where the agent is to be installed.

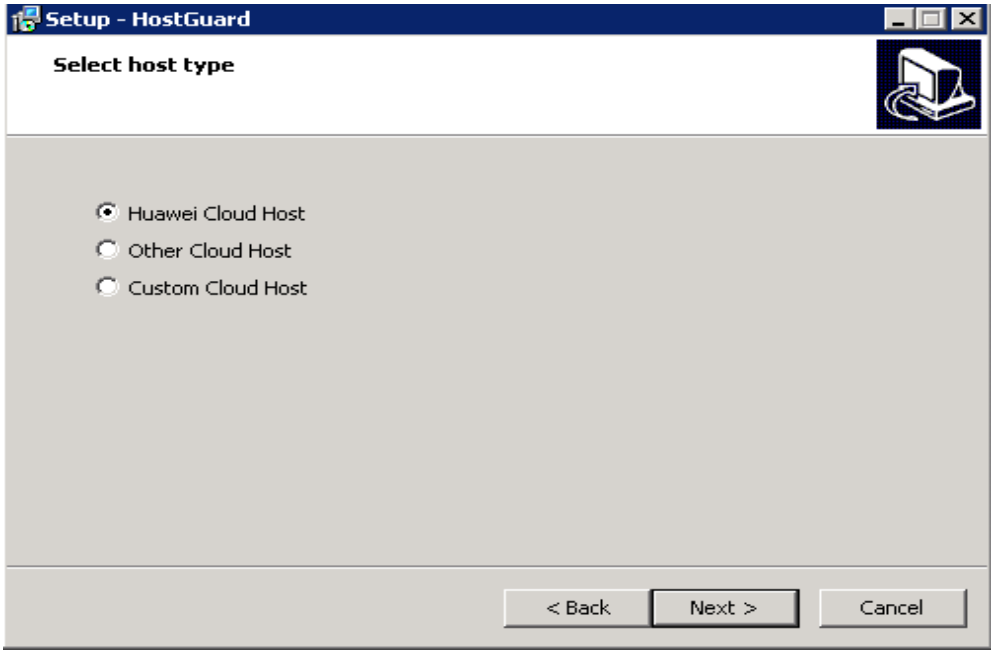
Step 6 Run the agent installation program as an administrator.

Select a host type on the **Select host type** page.

- HUAWEI CLOUD server: Select **Huawei Cloud Host**.

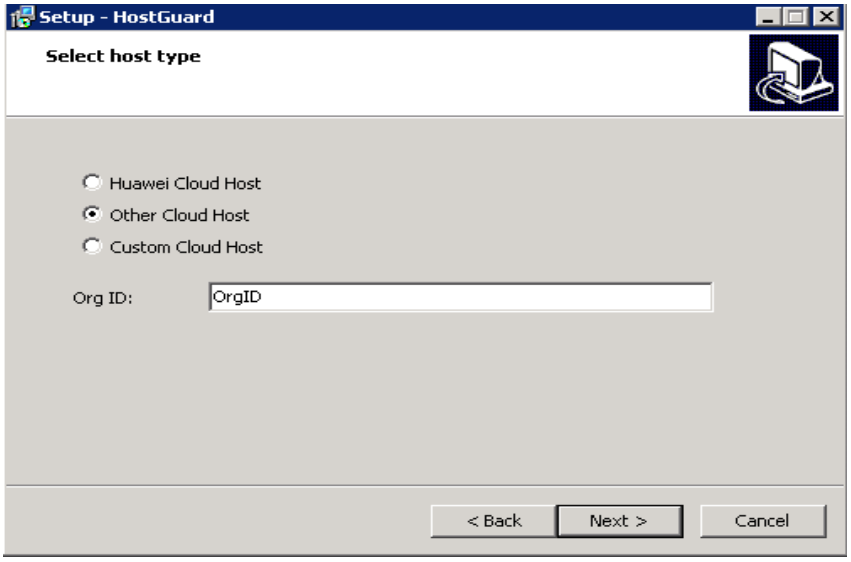
 Copyright © Huawei Technologies Co., Ltd.

Figure 1-8 Selecting a host type (HUAWEI CLOUD server)



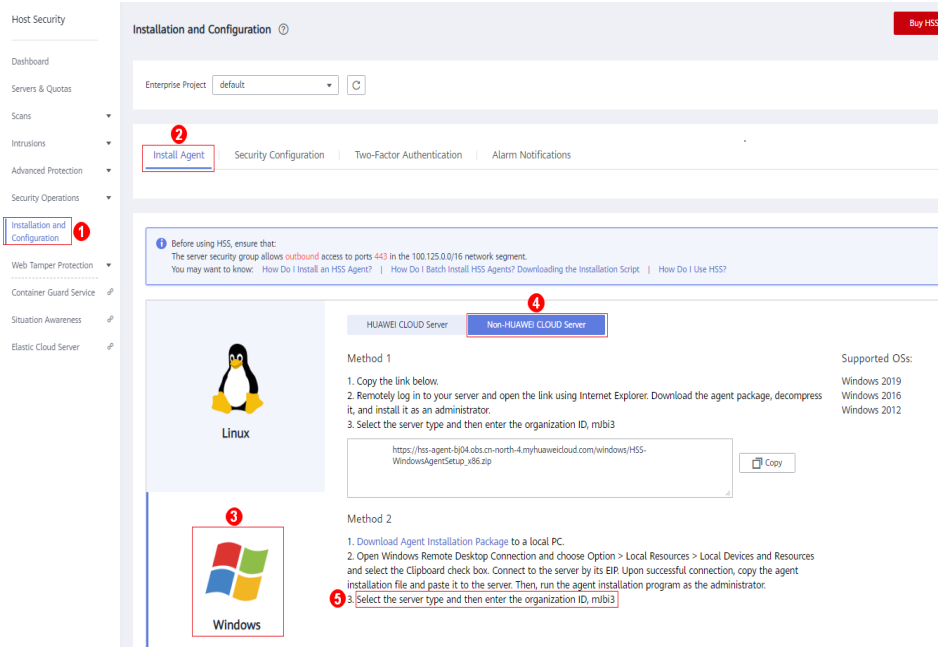
- Non-HUAWEI CLOUD server: Select **Other Cloud Host**. Copy the value of **Org ID** from the agent installation page, as shown in **Figure 1-10**.

Figure 1-9 Selecting a host type (non-HUAWEI CLOUD server)



Copyright © Huawei Technologies Co., Ltd.

Figure 1-10 Obtaining an organization ID (for a non-Huawei cloud server)

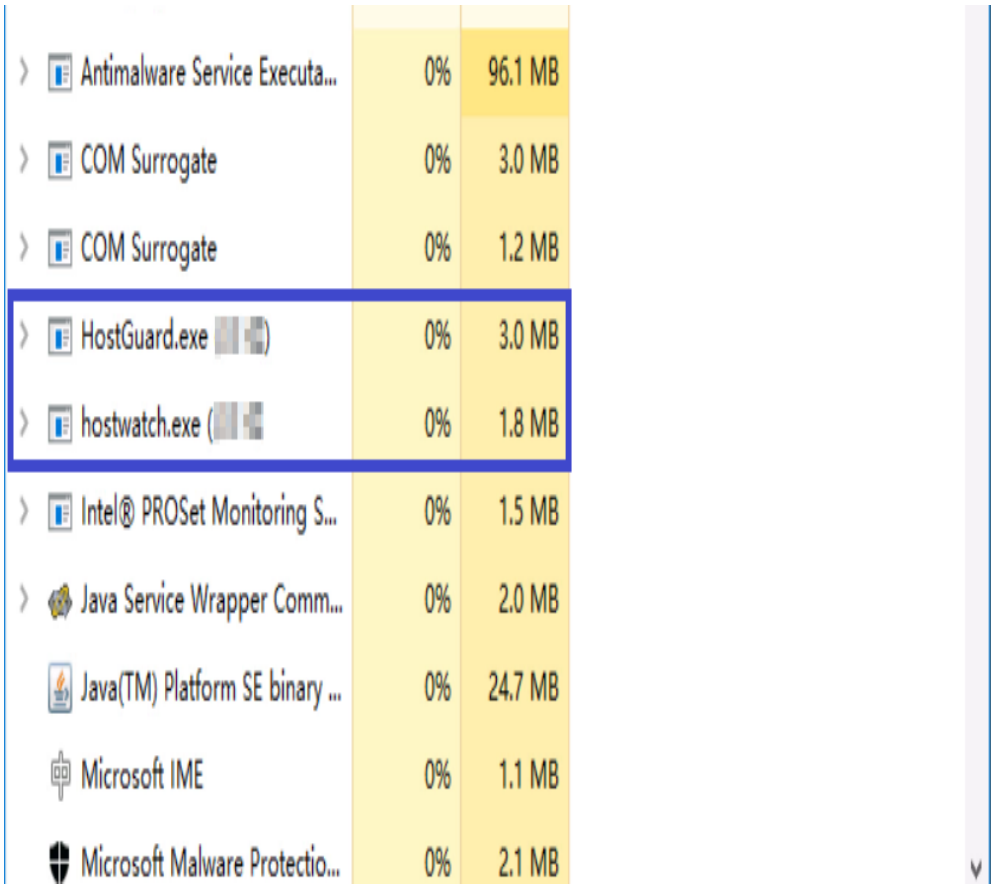


Step 7 Check the **HostGuard.exe** and **HostWatch.exe** processes in the Windows Task Manager.

If the processes do not exist, the agent installation fails. In this case, reinstall the agent.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-11 Checking the agent status



----End

Follow-Up Procedure

- For details about the agent status and troubleshooting, see **What Should I Do When the Agent Running Status Is Abnormal?**
- For details about handling agent installation failures, see **What Should I Do If Agent Installation Failed?**
- For details about agent uninstallation, see **How Do I Uninstall the Agent?**

1.3 (Optional) Step 3: Set Alarm Notifications

1.3.1 Enabling the Basic/Enterprise/Premium Edition

After alarm notification is enabled, you can receive alarm notifications sent by HSS to learn about security risks facing your servers and web pages. Without this function, you have to log in to the management console to view alarms.

If you do not set alarm notifications, the system will pop up a dialog box to remind you.

To hide this dialog box, click **Set Now** or select **Do not show again** and click **Ignore**.

- Alarm notification settings are effective only for the current region. To receive notifications from another region, switch to that region and configure alarm notification.
- Alarm notifications may be mistakenly intercepted. If you do not receive any alarm notifications, view them in the message interception area.
- The Simple Message Notification (SMN) service is a paid service. For details about the price, see **Product Pricing Details**.

Why Do I Need Alarm Notifications?

After the alarm notification function is enabled, HSS will send alarm information via SMS messages to your mobile devices immediately when alarms (on suspicious accounts, unknown ports, vulnerabilities, brute-force attacks, viruses, malicious programs, abnormal shells, web page tampering, ransomware, and so on) are reported. In this way, you can check alarms anytime anywhere and take measures, for example, enhance security, fix vulnerabilities, and manual scan for and kill viruses.

Prerequisites

Before you configure alarm notification,

- If you select **Use Message Center settings**, to set recipients, go to the Message Center and choose **Message Receiving Management** > **SMS & Email Settings**. In the **Security** area, click **Modify** in the row where **Security event** resides.
- If you select **Use SMN topic settings**, you are advised to create a message topic in the SMN service as an administrator. For details, see **Publishing a Message**.

NOTE

You can use Message Center settings or SMN topic settings for alarm notifications.

If you use Message Center settings, alarm notifications will be sent to the recipients specified in the **Security events** message type.

If you use SMN topic settings, you can create a topic and specify recipients for HSS.

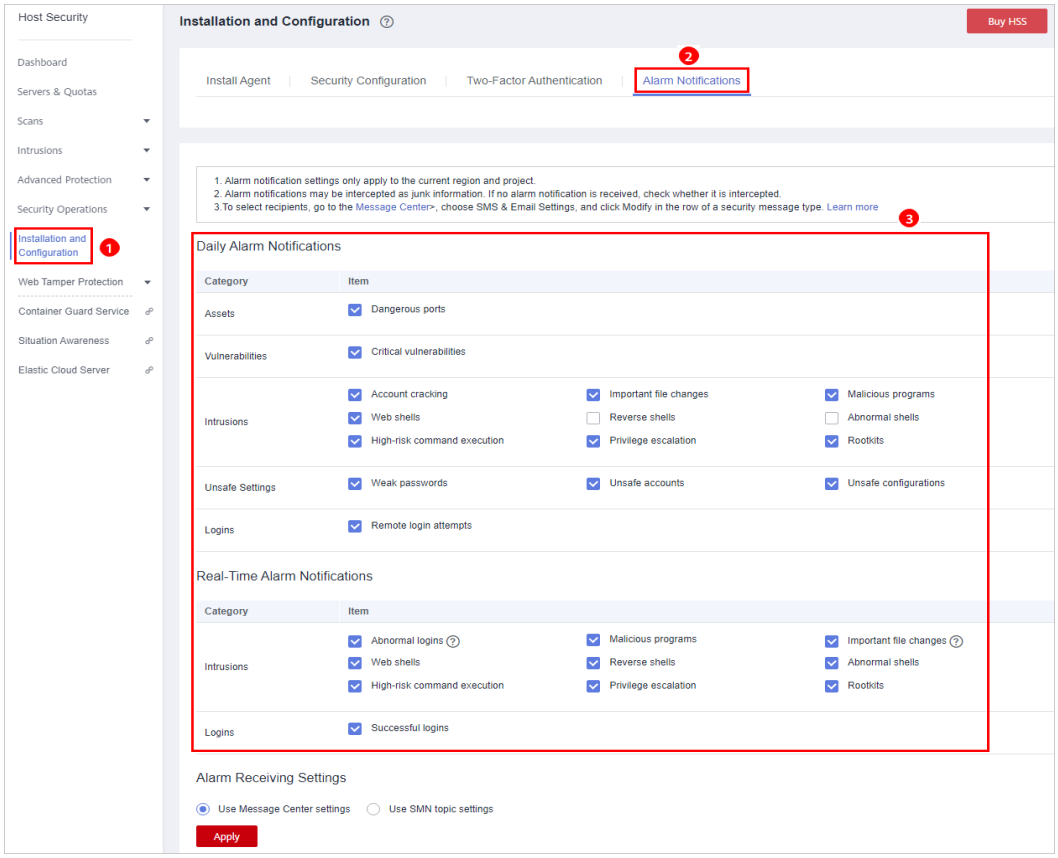
Enabling Alarm Notification for the Basic, Enterprise, or Premium Edition

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the displayed page, click the **Alarm Notifications** tab.

Figure 1-12 Basic/Enterprise/Premium edition



Step 4 Select the notification items for **Daily Alarm Notifications** and **Real-Time Alarm Notifications** as desired. For more information, see **Alarm Notifications**.

Table 1-2 Notification types

Notification Type	Description	Suggestion on Selecting a Notification Item
Daily alarm notification	The HSS system scans the accounts, web directories, vulnerabilities, malicious programs, and key configurations in the server system at 00:00 every day, and sends the summarized detection results to the recipients you set in the Message Center or SMN, whichever you enabled.	• It is recommended that you receive and periodically check all the content in the daily alarm notification to eliminate risks in a timely manner. • Daily alarm notifications contain a lot of check items. If you want to send the notifications to recipients set in an SMN topic, you are advised to set the topic protocol to **Email**.

 Copyright © Huawei Technologies Co., Ltd.

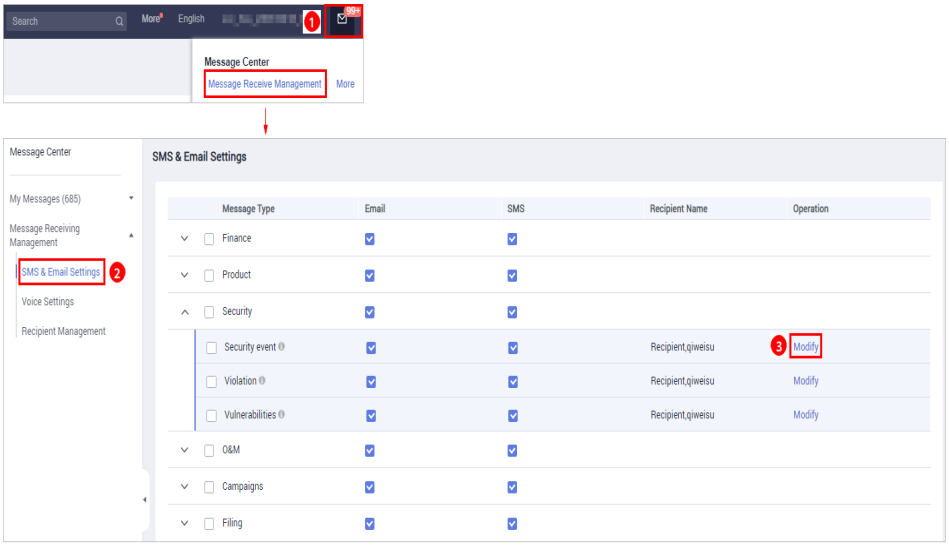
Notification Type	Description	Suggestion on Selecting a Notification Item
Real-time alarm notification	When an attacker intrudes a server, HSS sends alarms to the recipients you set in the Message Center or SMN, depending on which one you chose.	• It is recommended that you receive all the content in the real-time alarm notification and view them in time. The HSS system monitors the security of servers in real time, detects the attacker's intrusion, and sends real-time alarm notifications for you to quickly handle the problem. • Real-time alarm notifications are about urgent issues. If you want to send the notifications to recipients set in an SMN topic, you are advised to set the topic protocol to **SMS**.

Step 5 Select **Use Message Center settings** or **Use SMN topic settings**.

- Message Center settings

  Go to the Message Center and choose **Message Receiving Management** > **SMS & Email Settings**. In the **Security** area, click **Modify** in the row where **Security event** resides.

  Figure 1-13 Adding or modifying recipients



- SMN topic settings

  Select an available topic from the drop-down list or click **View Topics** and create a topic.

 Copyright © Huawei Technologies Co., Ltd.

To create a topic, that is, to configure a mobile phone number or email address for receiving alarm notifications, perform the following steps:

a. Follow the instructions described in **Creating a Topic** to create a topic.

b. Configure the mobile phone number or email address for receiving alarm notifications, that is, add one or more subscriptions for the created topic. For details, see **Adding a Subscription**.

c. Confirm the subscription. After the subscription is added, confirm the subscription as prompted by the received SMS message or email.

   The confirmation message about topic subscription may be regarded as spam. If you do not receive the message, check whether it is intercepted as spam.

You can create multiple notification topics based on the O&M plan and alarm notification type to receive different types of alarm notifications. For details about topics and subscriptions, see the *Simple Message Notification User Guide*.

Step 6 Click **Apply**. A message will be displayed indicating that the alarm notification is set successfully.

----End

Alarm Notifications

Notification Type	Item	Description
Daily Alarm Notifications HSS checks risks in your servers in the early morning every day, summarizes and collects detection results, and sends the results to your mobile phone or email box at 10:00 every day.		
Assets	Dangerous port	Check for high-risk open ports and unnecessary ports.
Vulnerabilities	Critical vulnerabilities	Detect critical vulnerabilities and fix them in a timely manner.
Intrusions	Account cracking	Detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts. ● If the number of brute-force attacks (consecutive incorrect password attempts) from an IP address reaches 5 within 30 seconds, the IP address will be blocked. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. ● You can check whether the IP address is trustworthy based on its attack type and how many times it has been blocked. You can manually unblock the IP addresses you trust.

 Copyright © Huawei Technologies Co., Ltd.

Notification Type	Item	Description
	Important file changes	HSS only checks whether directories or files have been modified, not whether they are modified manually or by a process.
	Malicious programs	Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants, and kill them in one click. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing.
	Web shells	Check whether the files (often PHP and JSP files) in your web directories are web shells.
	Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections.
	Abnormal shells	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.
	High-risk command execution	HSS checks executed commands in real time and generates alarms if high-risk commands are detected.
	Privilege escalation	HSS detects privilege escalation for processes and files in the current system.
	Rootkits	HSS detects suspicious rootkit installation in a timely manner by checking:
Unsafe Settings	Weak passwords	Detect weak passwords in MySQL, FTP, and system accounts.
	Unsafe accounts	Check for suspicious and unnecessary accounts on the servers to prevent unauthorized access and operations.
	Unsafe configurations	Detect unsafe settings of key applications that will probably be exploited by hackers to intrude servers.
Logins	Remote login attempts	Check and handle remote logins. If a user's login location is not any common login location you set, an alarm will be triggered.
Real-Time Alarm Notifications When an event occurs, an alarm notification is immediately sent.		

Notification Type	Item	Description
Intrusions	Abnormal logins	Detect abnormal login behavior, such as remote login and brute-force attacks. If abnormal logins are reported, your servers may have been intruded by hackers.
	Malicious programs	Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants, and kill them in one click. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing.
	Important file changes	HSS only checks whether directories or files have been modified, not whether they are modified manually or by a process.
	Web shells	Check whether the files (often PHP and JSP files) in your web directories are web shells.
	Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections.
	Abnormal shells	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.
	High-risk command execution	HSS checks executed commands in real time and generates alarms if high-risk commands are detected.
	Privilege escalation	HSS detects privilege escalation for processes and files in the current system.
	Rootkits	HSS detects suspicious rootkit installation in a timely manner by checking:

 Copyright © Huawei Technologies Co., Ltd.

Notification Type	Item	Description
Logins	Successful logins	This alarm does not necessarily indicate a security issue. If you have selected **Successful logins** in the **Real-Time Alarm Notifications** area, HSS will send alarms when detecting any successful logins. If all the accounts on your HSS are managed by a single administrator, such alarms help them conveniently monitor system accounts. If the system accounts are managed by multiple administrators, or different servers are managed by different administrators, too many alarms will interrupt O&M personnel. In this case, you are advised to disable the alarm item. **NOTE** Alarms on this event do not necessarily indicate attacks. Logins from valid IP addresses are not attacks.

1.3.2 Enabling Alarm Notification for the WTP Edition

After alarm notification is enabled, you can receive alarm notifications sent by HSS to learn about security risks facing your servers and web pages. Without this function, you have to log in to the management console to view alarms.

Prerequisites

Before you configure alarm notification,

- If you select **Use Message Center settings**, to set recipients, go to the Message Center and choose **Message Receiving Management** > **SMS & Email Settings**. In the **Security** area, click **Modify** in the row where **Security event** resides.
- If you select **Use SMN topic settings**, you are advised to create a message topic in the SMN service as an administrator. For details, see **Publishing a Message**.

NOTE

You can use Message Center settings or SMN topic settings for alarm notifications.

If you use Message Center settings, alarm notifications will be sent to the recipients specified in the **Security events** message type.

If you use SMN topic settings, you can create a topic and specify recipients for HSS.

Why Do I Need Alarm Notifications?

After the alarm notification function is enabled, HSS will send alarm information via SMS messages to your mobile devices immediately when alarms (on suspicious accounts, unknown ports, vulnerabilities, brute-force attacks, viruses, malicious programs, abnormal shells, web page tampering, ransomware, and so on) are reported. In this way, you can check alarms anytime anywhere and take measures,

for example, enhance security, fix vulnerabilities, and manual scan for and kill viruses.

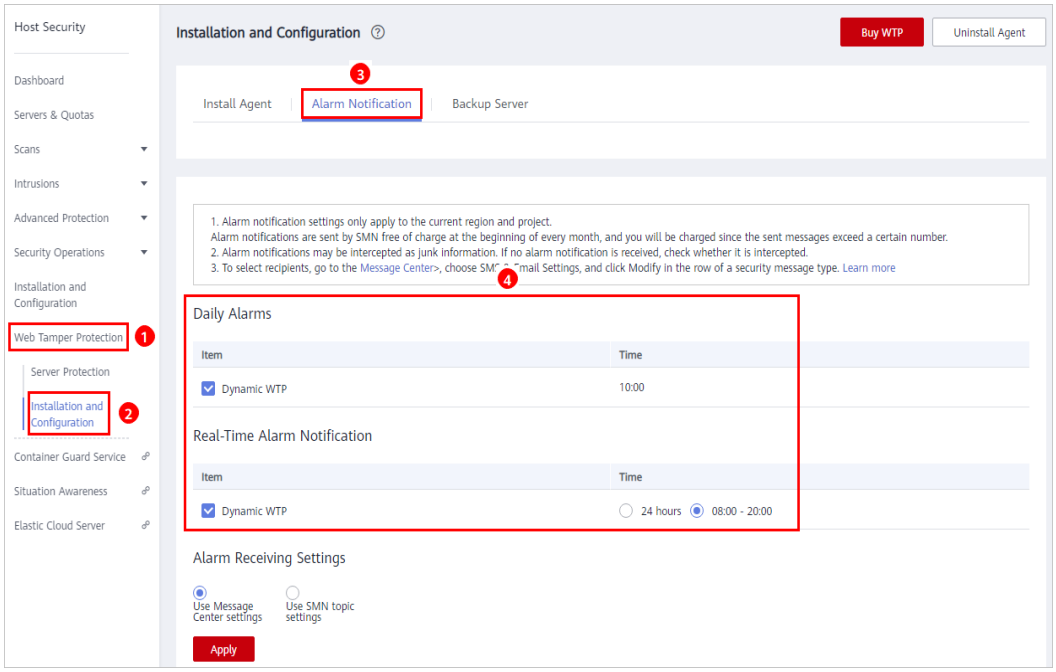
Enabling WTP Alarm Notifications

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Configure alarm time on the **Alarm Notification** tab of WTP.

Figure 1-14 Configuring alarm notifications



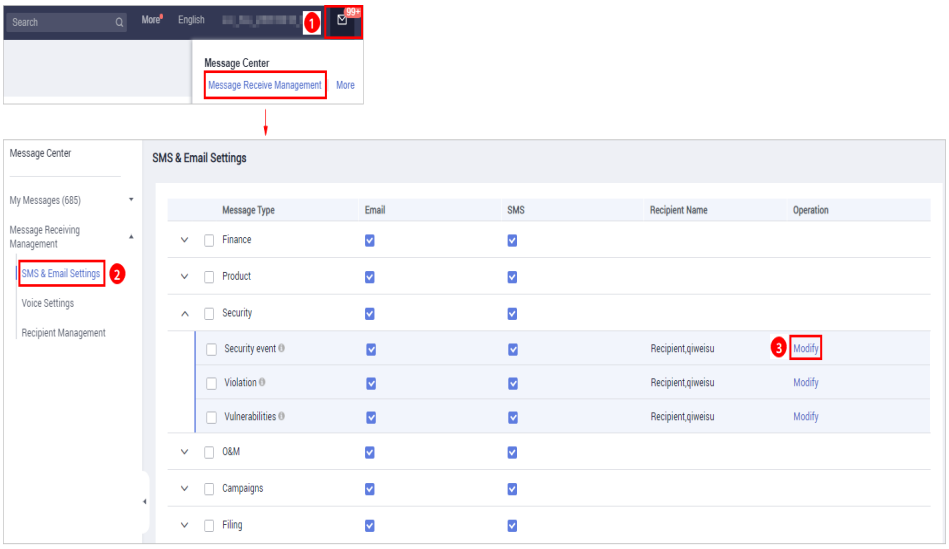
Step 4 Select **Use Message Center settings** or **Use SMN topic settings**.

- Message Center settings

  Go to the Message Center and choose **Message Receiving Management** > **SMS & Email Settings**. In the **Security** area, click **Modify** in the row where **Security event** resides.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-15 Adding or modifying recipients



- SMN topic settings

  Select an available topic from the drop-down list or click **View Topics** and create a topic.

  To create a topic, that is, to configure a mobile phone number or email address for receiving alarm notifications, perform the following steps:

  a. Follow the instructions described in **Creating a Topic** to create a topic.

  b. Configure the mobile phone number or email address for receiving alarm notifications, that is, add one or more subscriptions for the created topic. For details, see **Adding a Subscription**.

  c. Confirm the subscription. After the subscription is added, confirm the subscription as prompted by the received SMS message or email.

     The confirmation message about topic subscription may be regarded as spam. If you do not receive the message, check whether it is intercepted as spam.

  You can create multiple notification topics based on the O&M plan and alarm notification type to receive different types of alarm notifications. For details about topics and subscriptions, see the *Simple Message Notification User Guide*.

Step 5 Click **Apply**. A message will be displayed indicating that the alarm notification is set successfully.

----End

1.4 Step 4: Enable Server Protection

1.4.1 Enabling the Basic/Enterprise/Premium Edition

Before enabling HSS, you need to allocate a quota to a specified server. If the service is disabled or the server is deleted, the quota can be allocated to other servers.

 Copyright © Huawei Technologies Co., Ltd.

For the WTP edition, choose **Web Tamper Protection** > **Server Protection** and then enable it. For details, see **Enabling the WTP Edition**.

NOTE

- The basic edition can protect any number of servers, but only part of the security scan capabilities are available. This edition does not provide protection capabilities, nor does it provide support for DJCP MLPS certification.

  To protect your ECSs or pass the DJCP MLPS certification, purchase the enterprise edition or a higher edition (premium edition or Web Tamper Protection edition).
- The WTP edition can be enabled only on the **Server Protection** page of the WTP console. All the functions of the premium edition are included with the WTP edition.

Check Mode

The HSS system detects all data at 00:00 every day.

If you enable server protection before the detection interval, you can view detection results only after the detection is performed at 00:00 of the next day or you perform a manual detection immediately.

Prerequisites

- In the server list on the **Servers** page of the HSS console, the **Agent Status** of the target server is **Online**.
- You have purchased required edition quotas in your region.
- To better protect your containers, you are advised to **set security configurations**.

Restrictions

- Linux OS

  On servers running the EulerOS with ARM, HSS does not block the IP addresses suspected of SSH brute-force attacks, but only generates alarms.
- Windows OS
  - Authorize the Windows firewall when you enable protection for a Windows server. Do not disable the Windows firewall during the HSS in-service period. If the Windows firewall is disabled, HSS cannot block brute-force attack IP addresses.
  - If the Windows firewall is manually enabled, HSS may also fail to block brute-force attack IP addresses.

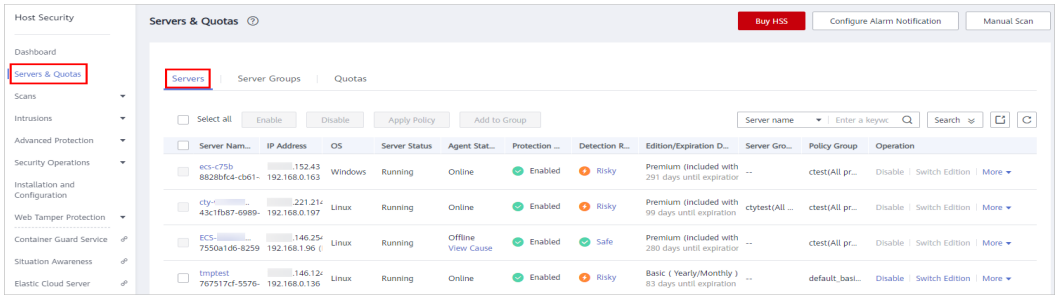
Enabling Protection

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation tree on the left, choose **Servers**.

Figure 1-16 Server list



NOTE

The server list displays the protection status of only the following servers:

- HUAWEI CLOUD servers purchased in the selected region
- Non-HUAWEI CLOUD servers that have been added to the selected region

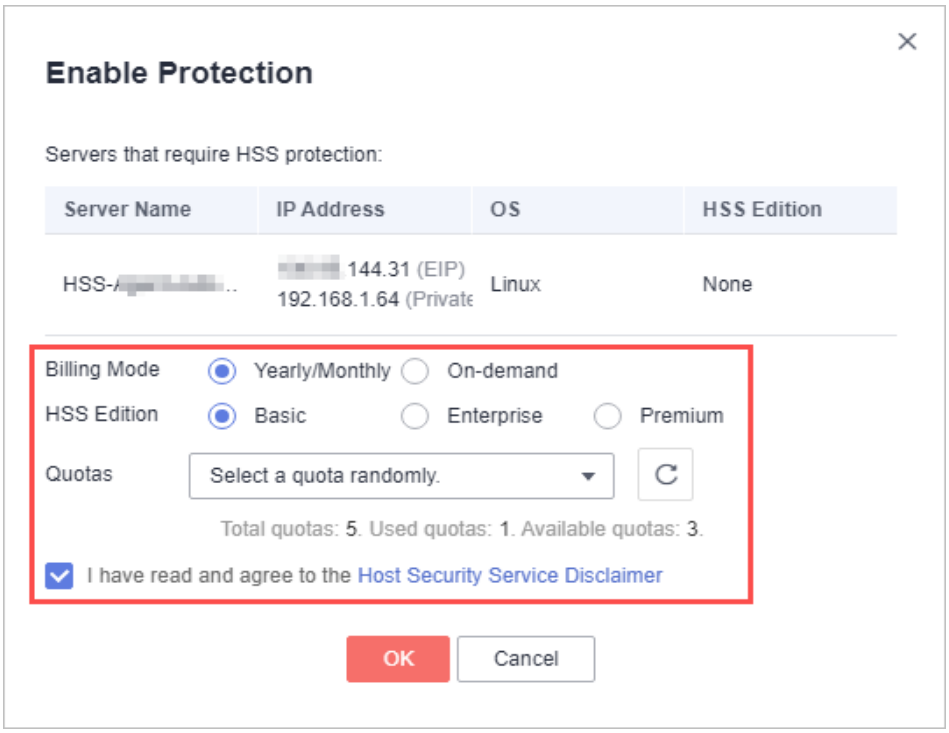
Step 4 Select the target server and click **Enable**.

You can buy HSS in pay-per-use or yearly/monthly mode.

- Yearly/Monthly

  In the displayed dialog box, select an edition, select the yearly/monthly mode, and allocate the HSS quota. Select **I have read and agree to the Host Security Service Disclaimer**.

Figure 1-17 Enabling yearly/monthly HSS



The quotas can be allocated in the following ways:

- Select **Select a quota randomly.** to let the system allocate the quota with the longest remaining validity to the server.

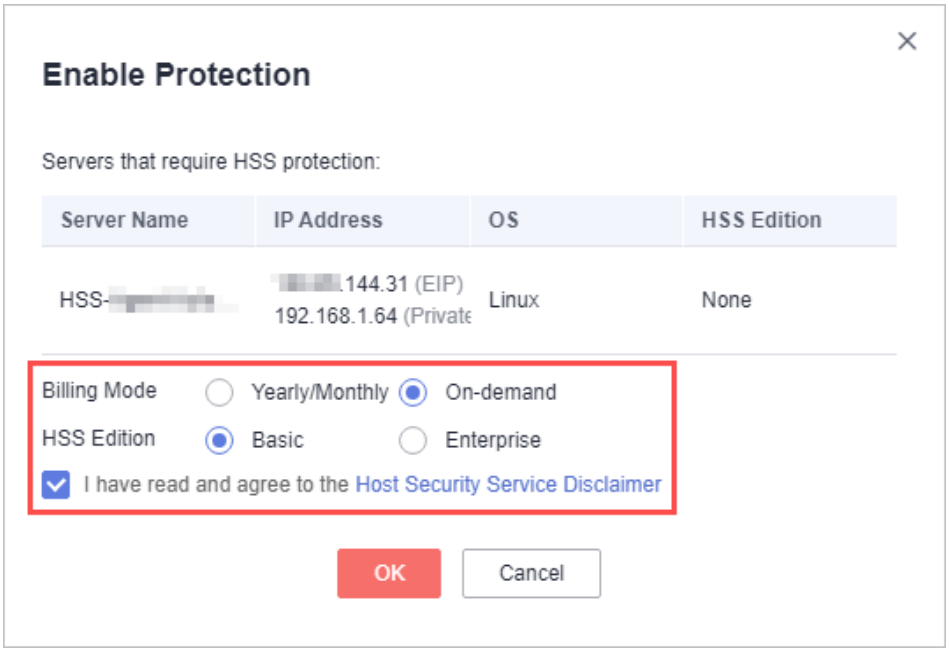
Copyright © Huawei Technologies Co., Ltd.

  - Select a quota to allocate.
  - Enable protection for servers in batches. The system will automatically allocate quota to them.

- Pay-per-use

  In the displayed dialog box, select the pay-per-use mode and the edition. Select **I have read and agree to the Host Security Service Disclaimer**.

  Figure 1-18 Enabling pay-per-use HSS



NOTE

Only the basic and enterprise editions support the pay-per-use mode. The basic edition can be used free of charge for 30 days. The yearly/monthly mode of the basic edition can be used only after purchase. For more information, see **Purchase HSS Quota**.

Step 5 Click **OK**. View the server protection status in the server list.

If the **Protection Status** of the target server is **Enabled**, the basic, enterprise, or premium edition has been enabled.

NOTE

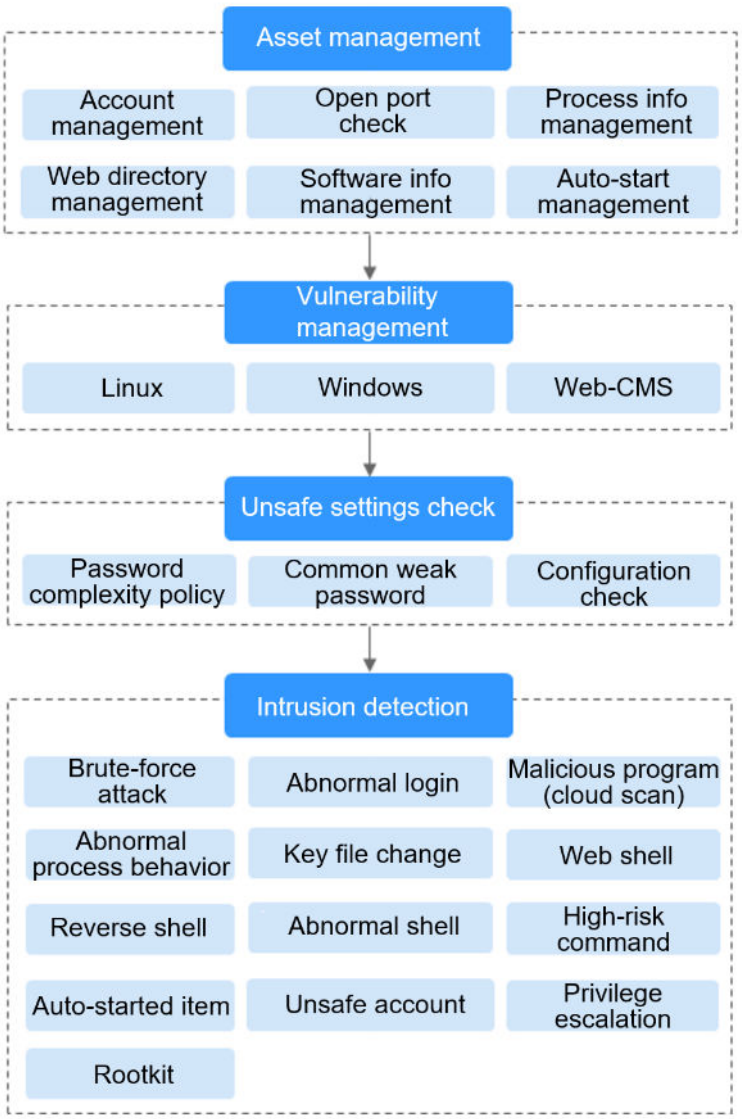
- Alternatively, on the **Quotas** tab of the **Servers** page, click **Bind Server** in the **Operation** column to bind a quota to a server. HSS will automatically enable protection for the server.
- A quota can be bound to a server to protect it, on condition that the agent on the server is online.

After HSS is enabled, it will scan your servers for security issues. Check items vary according to the edition you enabled. **Figure 1-19** illustrates more details.

For details about the differences between editions, see **Editions**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-19 Automatic security check items



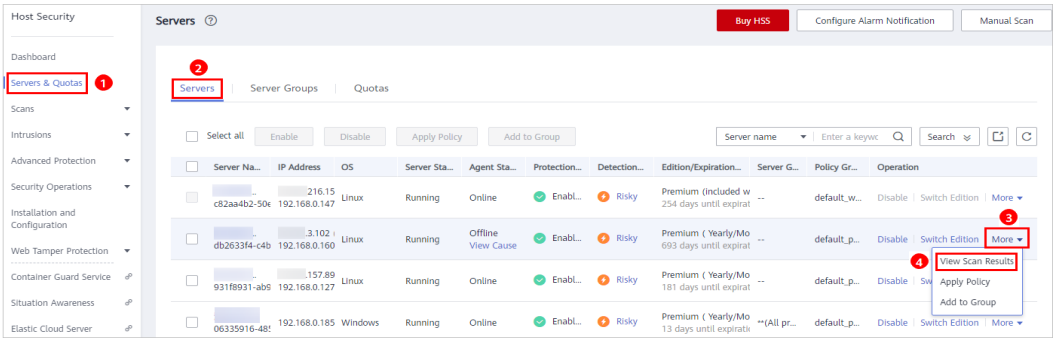
----End

Viewing Detection Details

After server protection is enabled, HSS will immediately perform comprehensive detection on the server. The detection may take a long time, which needs your patience.

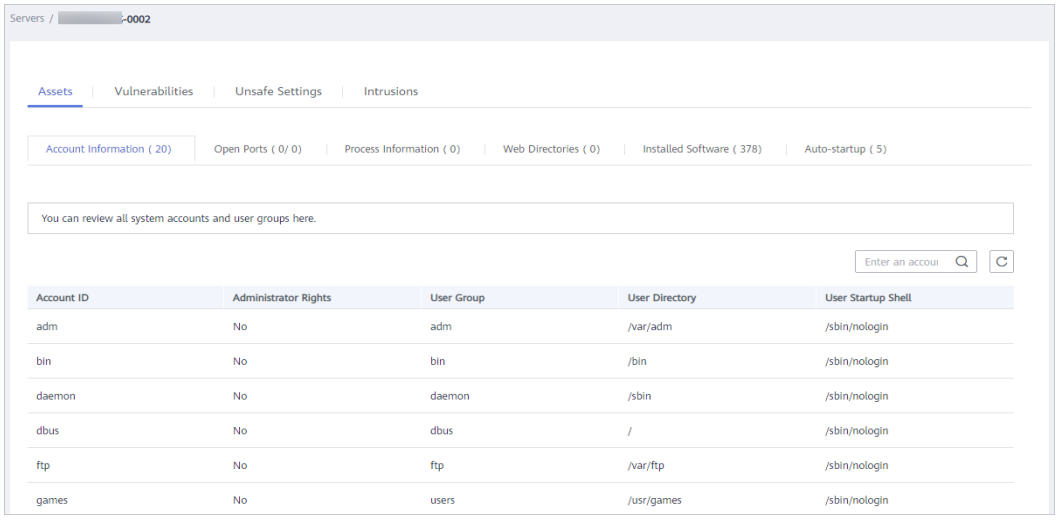
In the **Operation** column on the **Servers** tab, choose **More** > **View Scan Results** to view the detection result of a specified server.

Figure 1-20 Viewing details



The details page shows detection results and detected risks.

Figure 1-21 Viewing the detection result



Follow-up Operation

You can manually configure check items, as shown in **Figure 1-22**. Configurable items vary according to the edition you enabled.

For details about the differences between editions, see **Editions**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-22 Manual check items

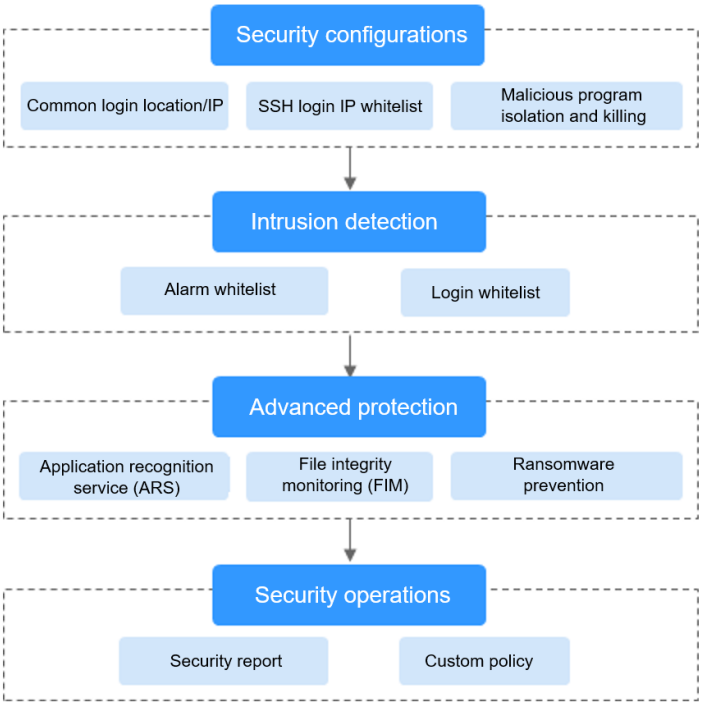


Table 1-3 Manual check items

Function	Check Item	Reference
Security configuration	• Common login location/IP address • SSH login IP address whitelist • Isolating and killing malicious programs	**Security Configuration**
Intrusion detection	• Alarm whitelist • Login whitelist	**Intrusion Detection**
Advanced protection	• Application recognition service (ARS) • File integrity monitoring (FIM) • Ransomware prevention	**Advanced Protection**
Security operations	• Security report • Custom policy management	**Security Operations**

Follow-Up Procedure

Disabling HSS

On the **Server** tab of the **Servers** page, click **Disable** in the **Operation** column of a server.

If HSS is disabled, HSS quota status will change from occupied to idle. You can allocate the idle quotas to other servers or unsubscribe the unnecessary quotas to prevent quota waste.

NOTICE

- Before disabling protection, perform a comprehensive detection on the server, handle known risks, and record operation information to prevent O&M errors and attacks on the server.
- After protection is disabled, clear important data on the server, stop important applications on the server, and disconnect the server from the external network to avoid unnecessary loss caused by attacks.

Unbinding quota

Choose **Servers** and click the **Quotas** tab. Locate a quota and choose **More** > **Unbind Quota** in the **Operation** column. If a quota is unbound, its status will change from **In use** to **Idle**, and it will no longer protect the servers bound to it.

You can allocate the idle quotas to other servers or unsubscribe the unnecessary quotas to prevent quota waste.

NOTE

If you unsubscribe from a cloud server protected by HSS, the server will not be automatically unbound from the HSS quota immediately. You can manually unbind it. The server will be automatically unbound from the HSS quota 30 days after the Agent goes offline.

1.4.2 Enabling the WTP Edition

Before enabling WTP, you need to allocate a quota to a specified server. If the service is disabled or the server is deleted, the quota can be allocated to other servers.

The premium edition will be enabled when you enable WTP.

 Copyright © Huawei Technologies Co., Ltd.

How WTP Prevents Web Page Tampering

Table 1-4 Protection mechanisms

Type	Mechanism
Static web page protection	1. Local directory lock WTP locks files in a web file directory in a drive to prevent attackers from modifying them. Website administrators can update the website content by using privileged processes. 2. Active backup and restoration If WTP detects that a file in a protected directory is tampered with, it immediately uses the backup file on the local host to restore the file. 3. Remote backup and restoration If a file directory or backup directory on the local host is invalid, you can use the remote backup service to restore the tampered web page.
Dynamic web page protection	1. Malicious behavior filtering based on RASP The runtime application self-protection (RASP) technologies developed by Huawei detect program behaviors, preventing attackers from tampering with web pages through application programs.

Restrictions

The Windows firewall must be enabled when you enable protection for a Windows server. Do not disable the Windows firewall during the HSS in-service period.

Prerequisites

- On the **Server Protection** page of the WTP console, the **Agent Status** of the target server is **Online**, and the **Protection Status** of the server is **Disabled**.
- In the server list on the **Servers** page of the HSS console, the **Agent Status** of the target server is **Online**, and the **Protection Status** of the server is **Disabled**.
- You have purchased sufficient quotas for the Web Tamper Protection edition in the selected region.

Setting Protected Directories

You can set:

- Directories

  You can add a maximum of 50 protected directories to a host. For details, see **Adding a Protected Directory or File System**.

  To record the running status of the server in real time, exclude the log files in the protected directory. You can grant high read and write permissions for log files to prevent attackers from viewing or tampering with the log files.

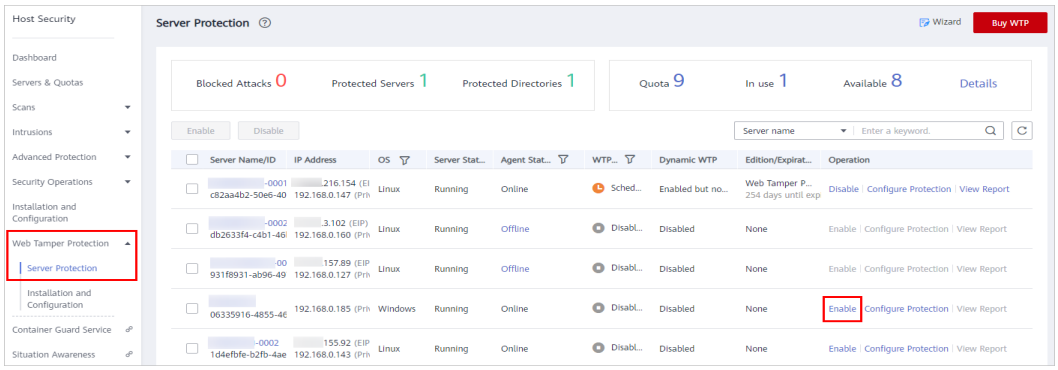
Enabling WTP

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Web Tamper Protection** > **Server Protection**. Click **Enable** in the **Operation** column of a server.

Figure 1-23 Web Tamper Protection



NOTE

The server list displays the protection status of only the following servers:

- HUAWEI CLOUD servers purchased in the selected region
- Non-HUAWEI CLOUD servers that have been added to the selected region

Step 4 In the **Enable WTP** dialog box, allocate quotas to servers and click **OK**, as shown in **Figure 1-24**.

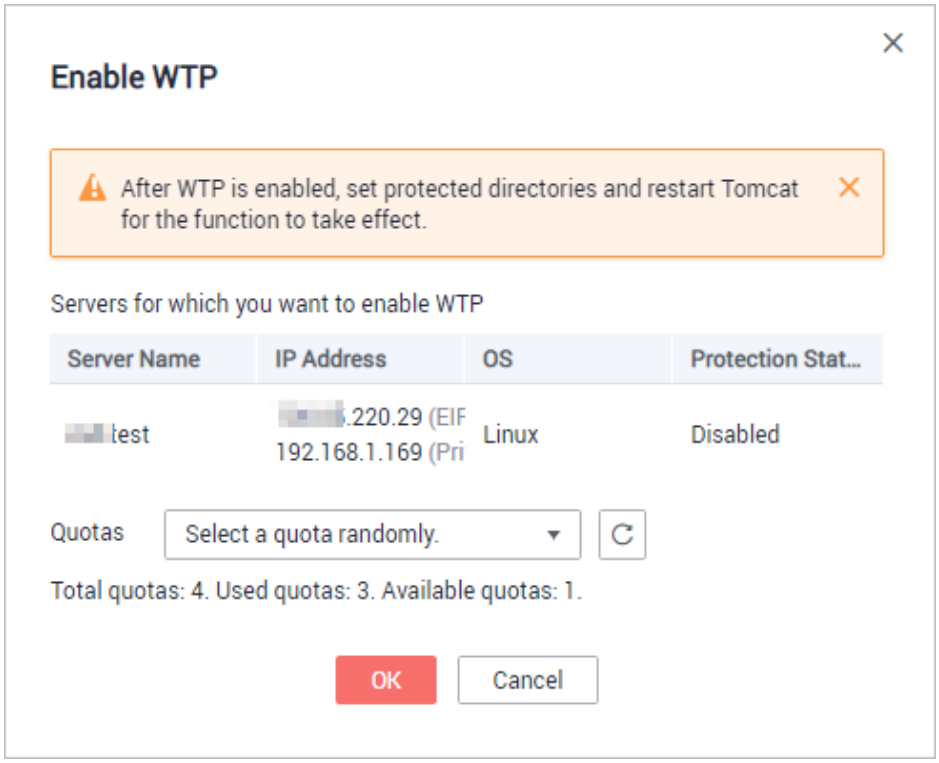
NOTE

If your server runs the Linux OS, you can enable WTP. After WTP is enabled, you need to restart Tomcat for the configuration to take effect.

If you have not enabled WTP, you can **enable it** later on the **Installation and Configuration** page.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-24 Enabling WTP



The quotas can be allocated in the following ways:

- Select **Select a quota randomly.** to let the system allocate the quota with the longest remaining validity to the server.
- Select a quota to allocate.
- Enable protection for servers in batches. The system will automatically allocate quota to them.

Step 5 View the server status on the **Web Tamper Protection** page.

The premium edition will be enabled when you enable WTP.

- Choose **Web Tamper Protection**, and click **Server Protection**. If the **WTP Status** of the target server is **Enabled** and the **Edition/Expiration Date** of it is **Web Tamper Protection**, the WTP edition is enabled.
- Choose **Host Security Service** > **Servers**, and choose **Servers**. If the **Protection Status** of the target server is **Enabled** and the **Edition/Expiration Date** of it is **Premium (included with WTP)**, the premium edition provided by the WTP edition is enabled free of charge.

----End

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

- To enable WTP protection for a server, you can also choose **Web Tamper Protection** > **Server Protection**, click **Details**, and click **Bind Server** in the **Operation** column of a quota.
- A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- Disable WTP before updating a website and enable it after the update is complete. Otherwise, the website will fail to be updated.
- Your website is not protected while WTP is disabled. Enable it immediately after updating your website.

Follow-Up Procedure

Disabling WTP

Choose **Web Tamper Protection** > **Server Protection** and click **Disable** in the **Operation** column of a server.

If WTP is disabled, its quota status will change from occupied to idle. You can allocate the idle quotas to other servers or unsubscribe the unnecessary quotas to avoid quota waste.

NOTICE

- Before disabling WTP, perform a comprehensive detection on the server, handle known risks, and record operation information to prevent O&M errors and attacks on the server.
- If WTP is disabled, web applications are more likely to be tampered with. Therefore, you need to delete important data on the server, stop important services on the server, and disconnect the server from the external network in a timely manner to avoid unnecessary losses caused by attacks on the server.
- After you or disable WTP, files in the protected directory are no longer protected. You are advised to process files in the protected directory before performing these operations.
- If you find some files missing after disabling WTP, search for them in the local or remote backup path.
- The premium edition will be disabled when you disable WTP.

Unbinding quota

To unbind a quota, choose **Web Tamper Protection** > **Server Protection**, click **Details**, and choose **More** > **Unbind Quota** in the **Operation** column of the quota. The quota status will change to **Idle**. HSS automatically disables WTP for servers associated with the quota.

You can allocate the idle quotas to other servers or unsubscribe the unnecessary quotas to prevent quota waste.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If you unsubscribe from a cloud server protected by WTP, the server will not be automatically unbound from the quota. You can manually unbind it. The server will be automatically unbound from the HSS quota 30 days after the Agent goes offline.

1.5 (Optional) Step 5: Switching the HSS Edition

You can switch the HSS edition to the basic edition (pay-per-use or yearly/monthly), enterprise edition (pay-per-use or yearly/monthly), or premium edition.

NOTE

- HSS editions cannot be switched in batches.
- When purchasing a HUAWEI CLOUD ECS, you can select basic or enterprise edition HSS. HSS will install its agent on the ECS and enable the selected edition, billed in pay-per-use mode. You can change to the yearly/monthly billing mode by switching edition.

Precautions

- From pay-per-use to yearly/monthly

  A yearly/monthly package order will be generated for you. The yearly/monthly quota will be available immediately when you complete payment. To enable the yearly/monthly quota, choose **Servers**. In the **Operation** column of the required server, click **Enable**, and select the yearly/monthly quota.
- From yearly/monthly to pay-per-use

  Choose **Servers**. In the **Operation** column of the required server, click **Enable**, and select the on-demand quota.
- If the HSS service is switched from a higher edition to a lower edition, protected servers will be more vulnerable to attacks.
- You can switch from other editions to the basic, enterprise, or premium edition. To use the WTP edition, you need to purchase and enable it separately.

Preparing for the Edition Switch

- Choose **Host Security Service** > **Servers**. On the **Servers** tab, check to ensure the **Agent Status** of required server is **Online**, and protection has been enabled for the server.
- Purchase required yearly/monthly quotas.
- Before switching to a lower edition, check the server, handle known risks, and record operation information to prevent O&M errors and attacks.

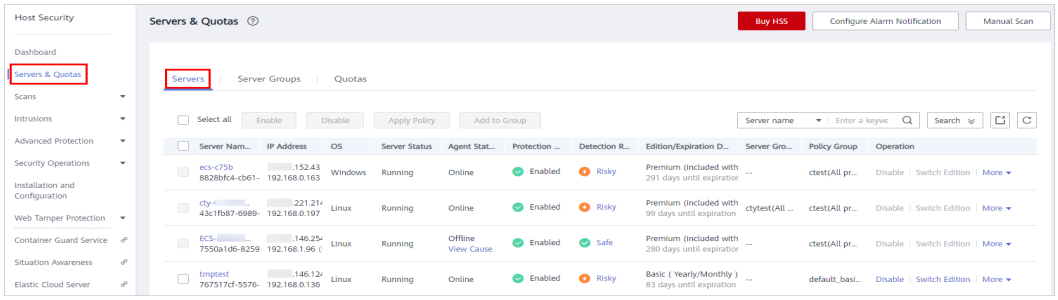
Switching Editions

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation tree on the left, choose **Servers**.

Figure 1-25 Server list



NOTE

The server list displays the protection status of only the following servers:

- HUAWEI CLOUD servers purchased in the selected region
- Non-HUAWEI CLOUD servers that have been added to the selected region

Step 4 In the **Operation** column of a server, click **Switch Edition**.

NOTE

- To switch between billing modes in the basic or enterprise edition, disable protection, and then choose the desired billing mode when you enable protection again.
- Clicking **Enable** in the **Operation** column of a server also lets you set an HSS edition.

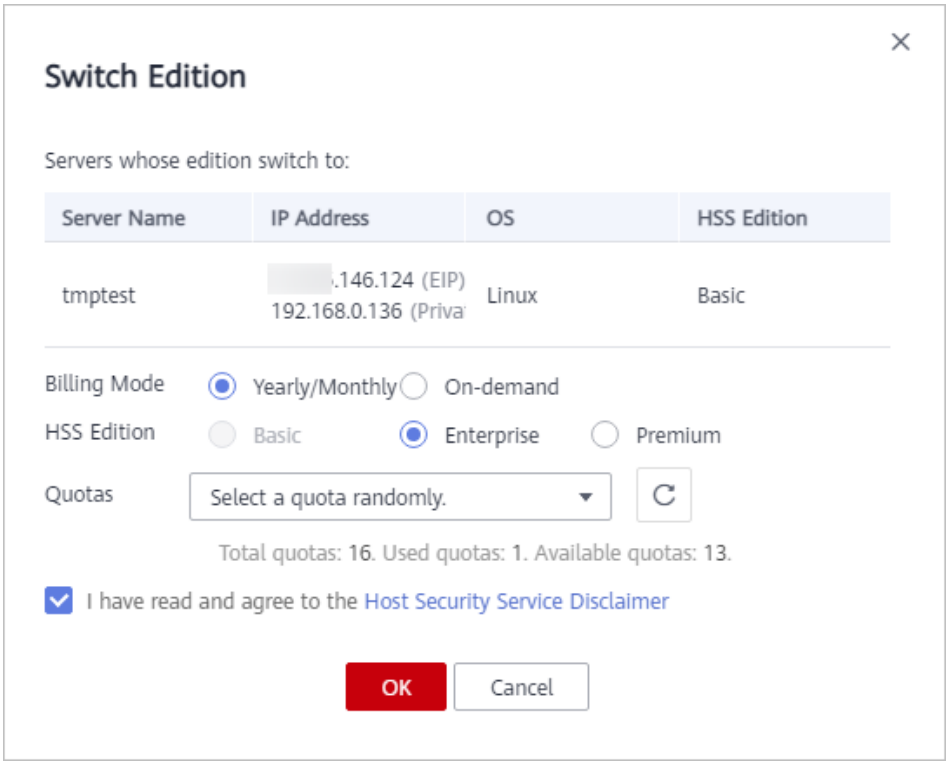
You can switch to an HSS edition in pay-per-use or yearly/monthly mode.

- Yearly/Monthly

  In the displayed dialog box, select an edition, select the yearly/monthly mode, and allocate the HSS quota. Select **I have read and agree to the Host Security Service Disclaimer**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-26 Switching to a yearly/monthly edition



The quotas can be allocated in the following ways:

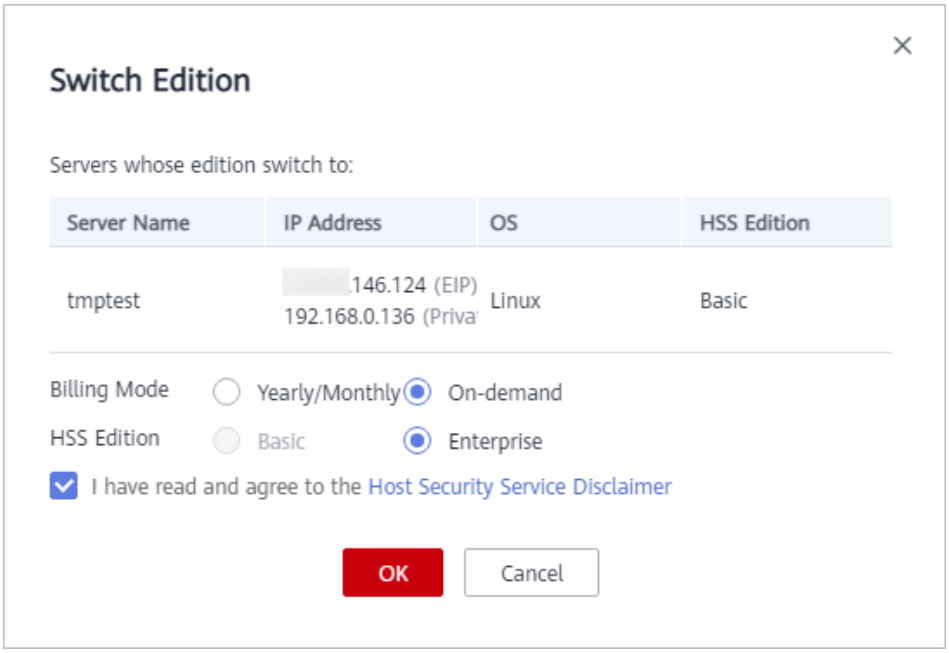
- Select **Select a quota randomly.** to let the system allocate the quota with the longest remaining validity to the server.
- Select a quota to allocate.
- Enable protection for servers in batches. The system will automatically allocate quota to them.

- Pay-per-use

  In the displayed dialog box, select **On-demand**, select an edition, and select **I have read and agree to the Host Security Service Disclaimer**, as shown in **Figure 1-27**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-27 Switching to a pay-per-use edition



Step 5 Click **OK**. The edition information in the **Edition/Expiration Date** column will be updated.

If the edition information in the **Edition/Expiration Date** column is updated, the edition switch succeeded.

----End

Follow-up Procedure

- After switching to a lower edition, clear important data on the server, stop important applications on the server, and disconnect the server from the external network to avoid unnecessary loss caused by attacks.
- After switching to a higher edition, **manually scan** your servers and handle detected problems.
- After the edition is switched, you can allocate the idle quotas to other servers or unsubscribe the unnecessary quotas to prevent quota waste.

Copyright © Huawei Technologies Co., Ltd.

2 Viewing the Server List

The server list on the **Servers** page displays the protection status of only the following servers:

- HUAWEI CLOUD servers purchased in the selected region
- Non-HUAWEI CLOUD servers that have been added to the selected region

NOTE

- Switch to the correct region before searching for your servers.
- If you have enabled the enterprise project function, you can select your enterprise project from the **Enterprise** project drop-down list to check server risk overview of the project.

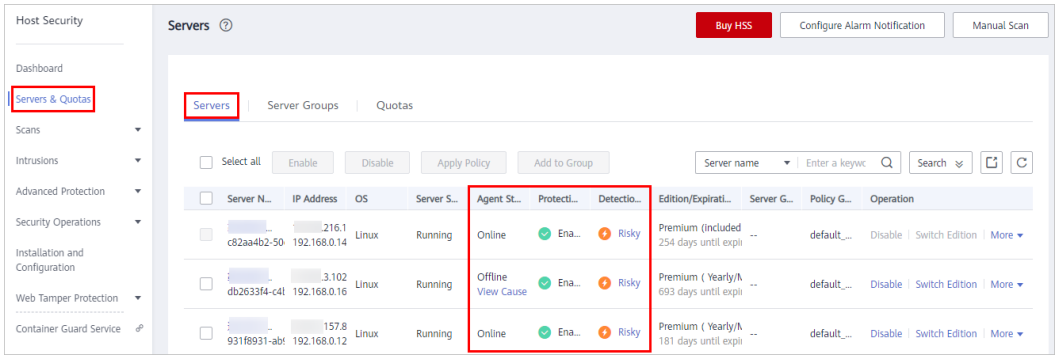
Viewing the Server List of the Basic/Enterprise/Premium Edition

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Servers** tab, check the protection status of servers.

Figure 2-1 Server list



 Copyright © Huawei Technologies Co., Ltd.

NOTE

- You can search for a server by its name, EIP, or private IP address.
- You can expand the advanced search area and search for a server by its name, ID, IP address, OS, agent status, protection status, detection result, policy group, server group, edition, server status, protection billing mode, or server billing mode.
- To export the server list, click .

Table 2-1 Statuses

Parameter	Description
Agent Status	• **Not installed**: The agent has not been installed or successfully started. Click **Install Agent** and install the agent as prompted. For details, see **Installing an Agent**. • **Online**: The agent is running properly. • **Offline**: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers. You can click **Offline**, and view servers whose agents are offline and the offline reasons at the bottom of the page that is displayed.
Protection Status	• **Enabled**: The server is fully protected by HSS. • **Disabled**: The server is not protected. If a server does not need protection, you can disable HSS for it to reduce its resource consumption.
Detection Result	• **Risky**: The host has risks. • **Safe**: No risks are found. • **Pending risk detection**: HSS is not enabled for the server.

----End

Viewing the WTP List

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

Step 2 In the upper left corner of the page, select a region, click , and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Web Tamper Protection** > **Server Protection**. Check the protection status of servers.

Figure 2-2 Server protection

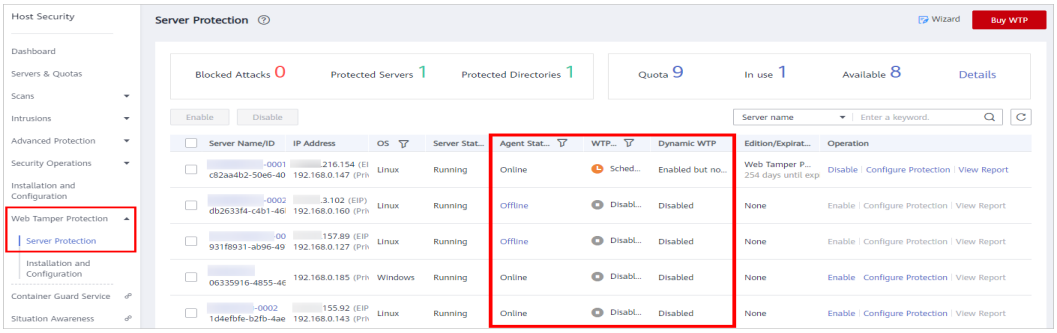


Table 2-2 Statuses

Parameter	Description
Agent Status	• **Not installed**: The agent has not been installed or successfully started. Click **Not installed** and install the agent as prompted. For details, see **Installing an Agent**. • **Online**: The agent is running properly. • **Offline**: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers. You can click **Offline**, and view servers whose agents are offline and the offline reasons at the bottom of the page that is displayed.
WTP Status	Status of static WTP, which can be: • **Enabled**: HSS provides static WTP for the server. • **Scheduled protection**: WTP is disabled for the server in a certain period. To set this period, click **Configure Protection** in the **Operation** column, and click the **Scheduled Protection** tab. For more information, see **Setting Scheduled WTP Protection**. • **Disabled**: The server is not protected. If a server does not need static WTP, you can disable HSS for it to reduce its resource consumption.
Dynamic WTP	Status of dynamic WTP, which can be: • **Enabled**: Dynamic WTP is enabled for the server. To enable dynamic WTP, click **Configure Protection** in the **Operation** column, and click the **Dynamic WTP** tab. For more information, see **Enabling Dynamic WTP**. • **Enabled but not in effect**: Dynamic WTP is enabled but has not taken effect. You need to restart Tomcat to make it take effect. • **Disabled**: Dynamic WTP is disabled.

----End

Copyright © Huawei Technologies Co., Ltd.

Helpful Links

- **Enabling the HSS Basic, Enterprise, or Premium Edition**
- **Enabling the WTP Edition**

Copyright © Huawei Technologies Co., Ltd.

3 Dashboard

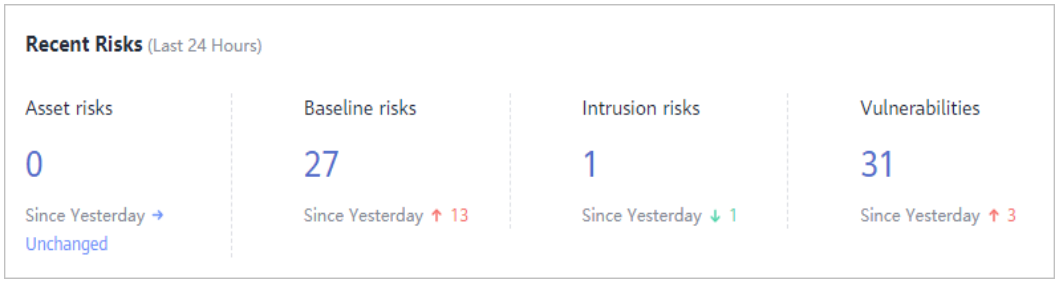
The **Dashboard** page displays server protection status, risk statistics on protected servers within the last 24 hours, and risk trend and top 5 vulnerable servers in the past seven days.

NOTE

If you have enabled the enterprise project function, you can select your enterprise project from the **Enterprise project** drop-down list to check server risk overview of the project. If you select **All projects**, the risk overview of servers in all the projects in this region is displayed.

Risk Statistics on Protected Servers (Last 24 Hours)

Figure 3-1 Risk statistics on protected servers (last 24 hours)



You can check the number of risks detected for protected servers over the past 24 hours.

You can click the number to view details about each risk.

 Copyright © Huawei Technologies Co., Ltd.

Server Protection Status (Last 24 Hours)

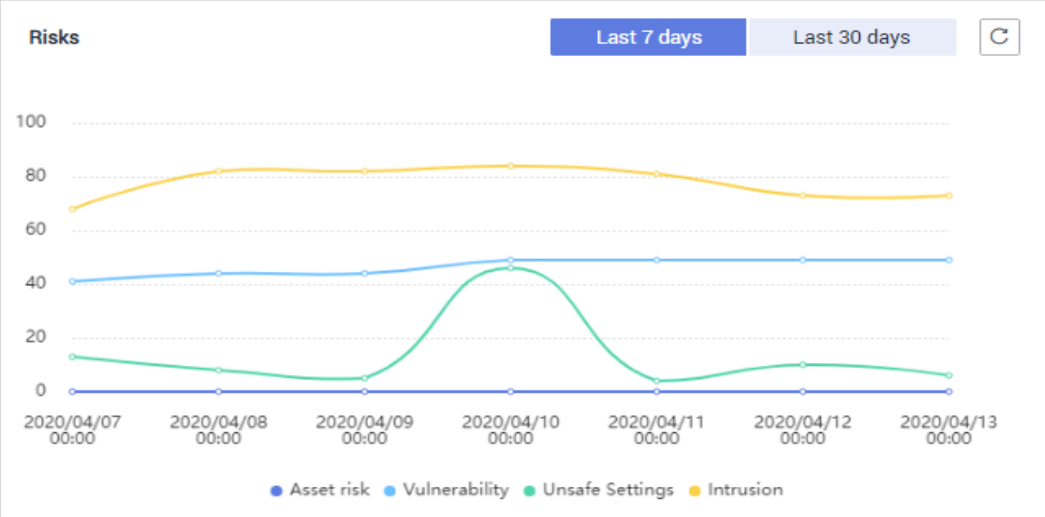
Figure 3-2 Server protection status

You can check the numbers of servers protected with the basic, enterprise, or premium edition and the number of unprotected servers.

To enable protection for required servers, click **Enable All**.

Risks

Figure 3-3 Risks



You can check risk statistics in the last 7 days or 30 days.

Table 3-1 Risks

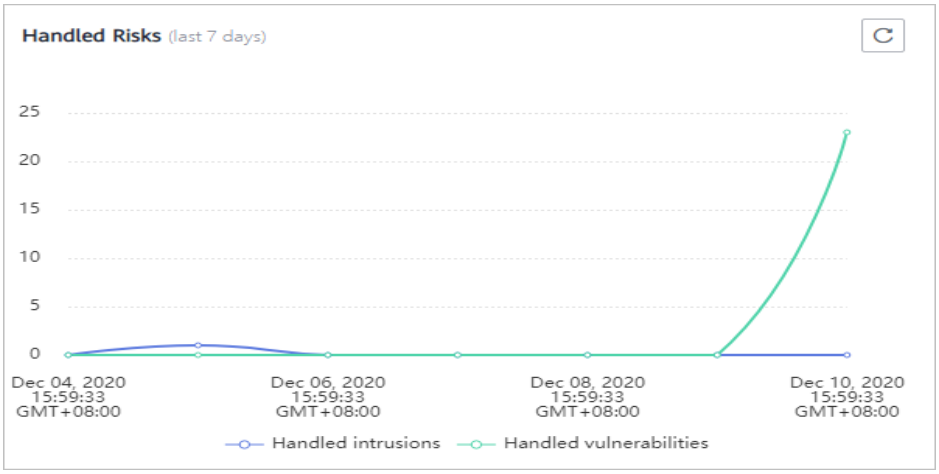
Category	Item
Asset	• Account • Open port • Process • Web directory • Software • Auto-startup

Copyright © Huawei Technologies Co., Ltd.

Category	Item
Vulnerability	• Linux vulnerability • Windows vulnerability • Web-CMS vulnerability
Unsafe setting	• Password complexity policy • Common weak password • Unsafe configuration item
Intrusion	• Attacker IP address • Abnormal shell • Malicious program • High-risk command • Abnormal process behavior • Auto-startup check • Abnormal login • Privilege escalation • Changes in critical file • High-risk malicious program • Rootkit • Web shell • Unsafe account • Reverse shell

Handled Risks (Last 7 Days)

Figure 3-4 Handled risks

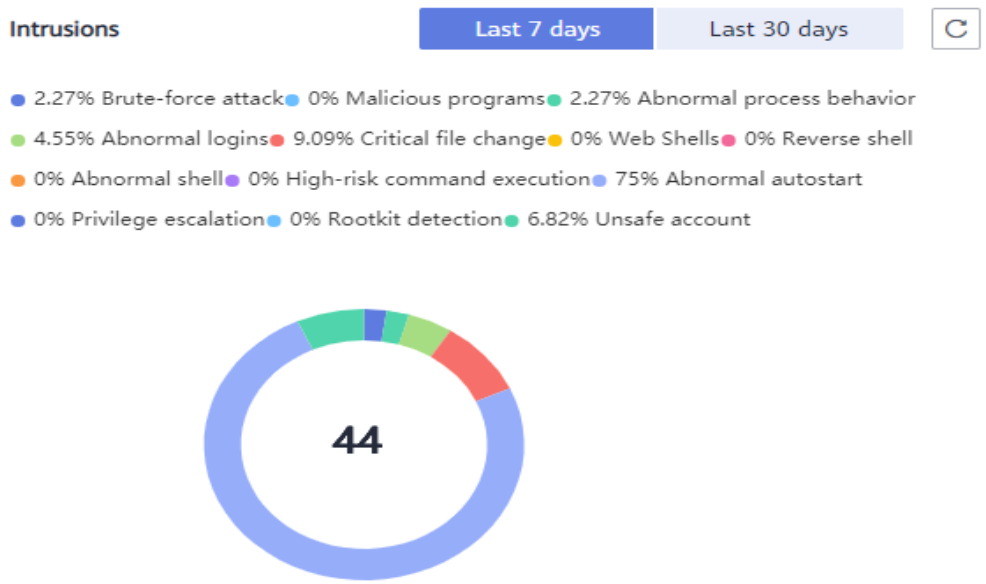


You can check the intrusions and vulnerabilities handled in the last seven days.

 Copyright © Huawei Technologies Co., Ltd.

Intrusions

Figure 3-5 Intrusions



You can check the numbers and types of intrusions in the last seven or 30 days.

These intrusion statistics are updated at 00:00 a.m. every day.

If no data is displayed due to connection problems, fix your network and click  to retrieve data again.

Top 5 Unsafe Servers (Last 7 Days)

Figure 3-6 Top 5 unsafe servers (last 7 days)

Copyright © Huawei Technologies Co., Ltd.

If you have enabled the basic, enterprise, or premium edition HSS, you can check the top 5 unsafe servers, which have the most risks detected in the past week, and the numbers of each type of risks.

At 00:00 every morning, server risks and the five servers with highest risks in the past seven days are updated.

If no data is displayed due to connection problems, fix your network and click  to retrieve data again.

Real-time Intrusions

Figure 3-7 Real-time intrusions

You can check the latest five intrusion events that have not been processed in the last 24 hours, including their alarm names, affected server names/IP addresses, description, occurrence time, and status.

- To check alarm details, click an alarm name.
- To handle an alarm, click **Handle** in the **Operation** column of the alarm. After the alarm is handled, it will be removed from the list. The list refreshes and displays the latest five intrusion events that have not been handled in the last seven days.
- To check more alarm events, click **View more** to go to the **Events** page.

4 Security Configuration

After protection is enabled, you can set security configurations, including common login locations, common login IP addresses, SSH login IP address whitelist, and the automatic isolation and killing of malicious programs.

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

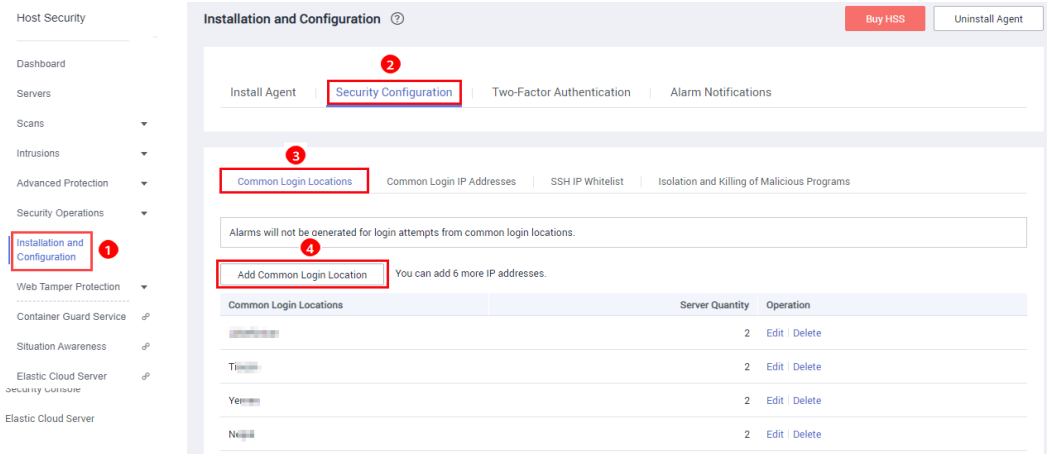
----End

Configuring Common Login Locations

After you configure common login locations, HSS will generate alarms on the logins from other login locations. A server can be added to multiple login locations.

Step 1 On the **Common Login Locations** tab, click **Add Common Login Location**.

Figure 4-1 Adding a common login location



Step 2 In the displayed dialog box, set the location and servers.

----End

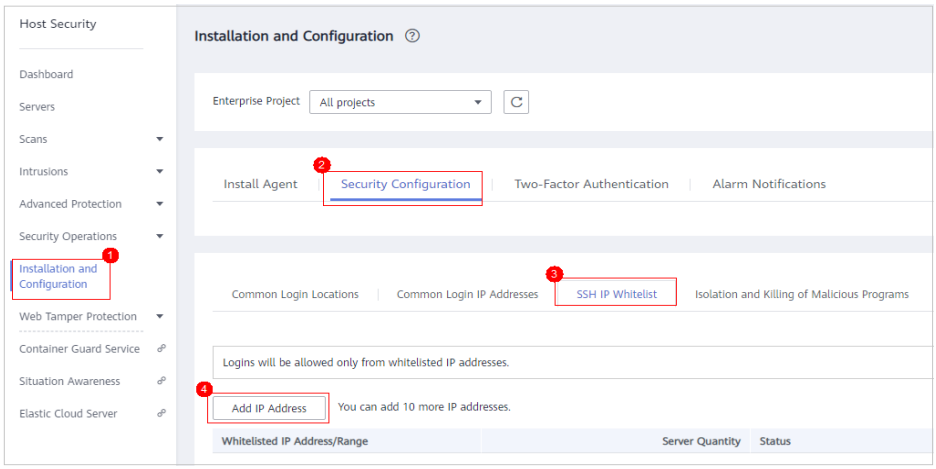
 Copyright © Huawei Technologies Co., Ltd.

Configuring Common Login IP Addresses

After you configure common IP addresses, HSS will generate alarms on the logins from other IP addresses.

Step 1 On the **Common Login IP Addresses** tab, click **Add Common Login IP Address**.

Figure 4-2 Adding a common login IP address



Step 2 In the displayed dialog box, set the login IP address and servers.

NOTE

A common login IP address must be a public IP address or IP address segment. Otherwise, you cannot remotely log in to the server in SSH mode.

----End

Configuring an SSH Login IP Address Whitelist

The SSH login whitelist controls SSH access to servers, effectively preventing account cracking.

After you configure an SSH login IP address whitelist, SSH logins will be allowed only from whitelisted IP addresses.

- Before enabling this function, ensure that all IP addresses that need to initiate SSH logins are added to the whitelist. Otherwise, you cannot remotely log in to your server using SSH.

  If your service needs to access a server, but not necessarily via SSH, you do not need to add its IP address to the whitelist.
- Exercise caution when adding an IP address to the whitelist. This will make HSS no longer restrict access from this IP address to your servers.

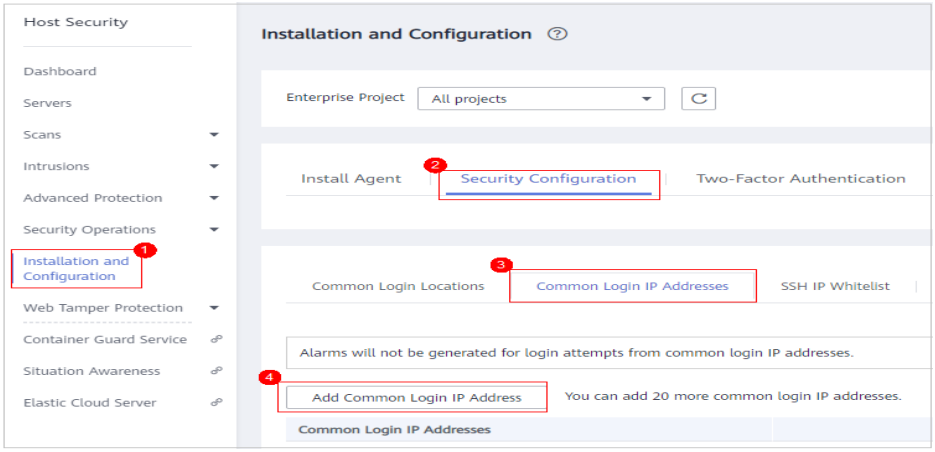
NOTE

The SSH IP address whitelist does not take effect for servers running Kunpeng EulerOS (EulerOS with ARM), or Centos 8.0 or later.

Step 1 On the **SSH IP Whitelist** tab, click **Add IP Address**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 Adding an SSH login IP address to whitelist



Step 2 In the **Add IP Address** dialog box, enter an IP address and select servers.

NOTE

A whitelisted IP address must be a public IP address or IP address segment (IPv4 and IPv6 addresses are supported). Otherwise, you cannot remotely log in to the server in SSH mode.

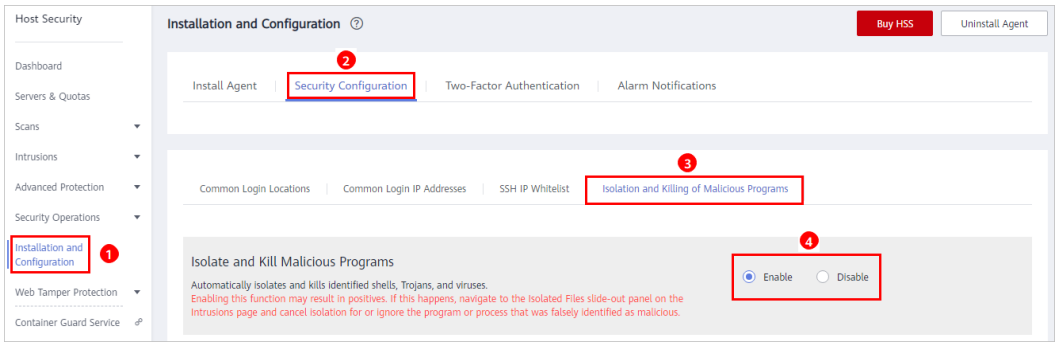
----End

Isolating and Killing Malicious Programs

HSS can automatically isolate and kill malicious programs, including web shells, Trojans, and worms. For more information, see **Intrusion Detection** > **Malicious Programs** in **Functions and Features**.

On the **Isolation and Killing of Malicious Programs** tab, select **Enable**.

Figure 4-4 Isolating and killing malicious programs



Automatic isolation and killing may cause false positives. You can choose **Intrusions** > **Events** to view isolated malicious programs. You can cancel the isolation or ignore misreported malicious programs. For details, see **Checking and Handling Intrusion Events**.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

- When a program is isolated and killed, the process of the program is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious programs (if any).
- If **Isolate and Kill Malicious Programs** is set to **Disable** on the **Isolation and Killing of Malicious Programs** tab, HSS will generate an alarm when it detects a malicious program.

  To isolate and kill the malicious programs that triggered alarms, choose **Intrusions** > **Events** and click **Malicious program (cloud scan)**.

Enabling 2FA

- 2FA requires users to provide verification codes before they log in. The codes will be sent to their mobile phones or email boxes.
- You have to choose an SMN topic for servers where 2FA is enabled. The topic specifies the recipients of login verification codes, and HSS will authenticate login users accordingly.

Prerequisites

- The enterprise, premium, or WTP edition of HSS has been enabled.
- You have created a message topic whose protocol is SMS or email.
- Server protection has been enabled.
- Linux servers require user passwords for login.
- To enable two-factor authentication, you need to disable the SELinux firewall.
- On a Windows server, 2FA may conflict with G01 and 360 Guard (server edition). You are advised to stop them.

Constraints and Limitations

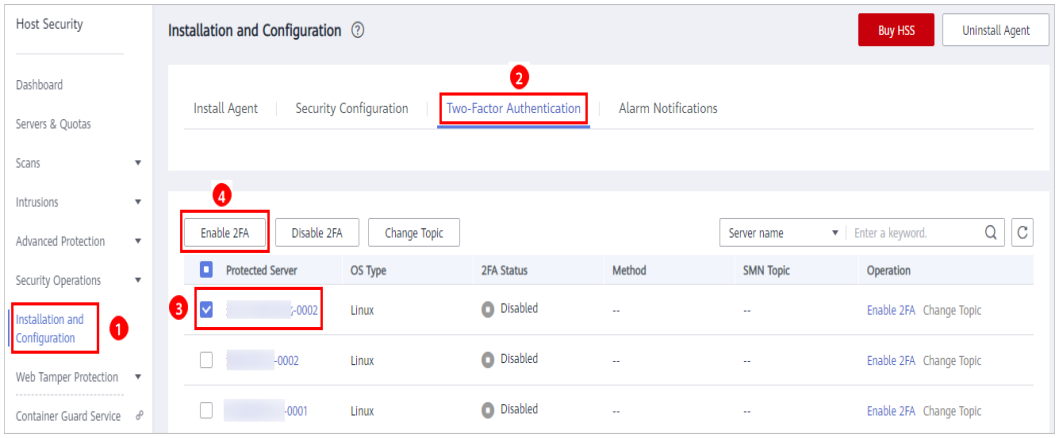
- If 2FA is enabled, you cannot log in to the servers running a GUI Linux OS.
- If you have enabled 2FA on a Linux server, you cannot log in to it through CBH.
- If you have enabled 2FA on a server, you cannot log in to the server through CloudShell.
- You can add up to 10 mobile numbers and email addresses at a time. A topic can have up to 10,000 mobile numbers and email addresses.

Procedure

Step 1 On the **Two-Factor Authentication** tab, click **Enable 2FA**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-5 2FA



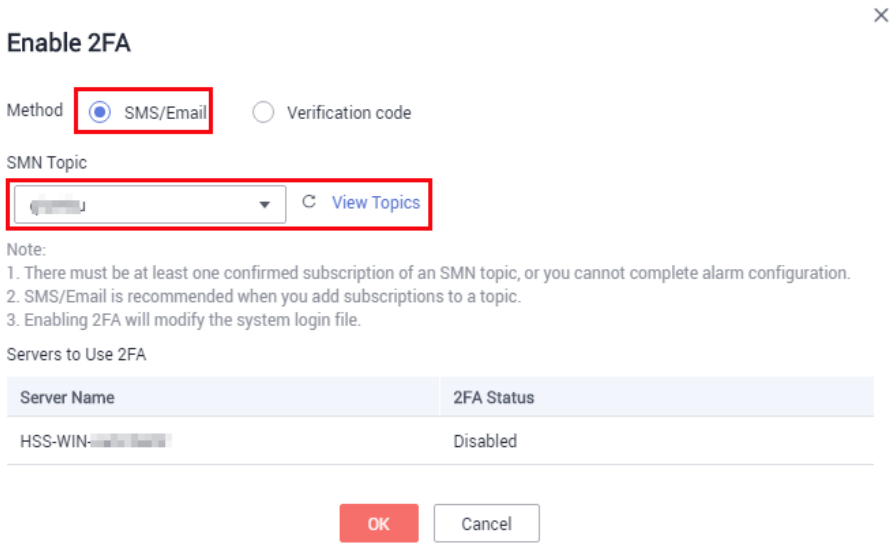
Step 2 In the displayed **Enable 2FA** dialog box, select an authentication mode.

- **SMS/Email**

  You need to select an SMN topic for SMS and email verification.

  - The drop-down list displays only notification topics that have been confirmed.
  - If there is no topic, click **View** to create one. For details, see **Creating a Topic**.
  - During authentication, all the mobile numbers and email addresses specified in the topic will receive a verification SMS or email. You can delete mobile numbers and email addresses that do not need to receive verification messages.

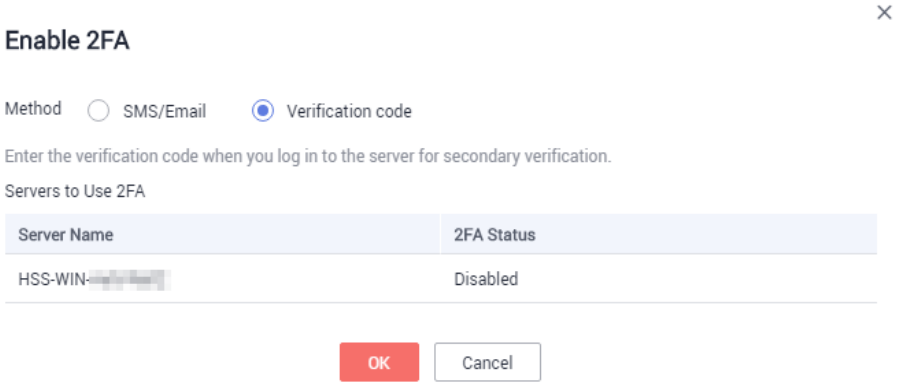
  Figure 4-6 SMS/Email



- **Verification code**

Copyright © Huawei Technologies Co., Ltd.

Figure 4-7 Verification code



Step 3 Click **OK**. After 2FA is enabled, it takes about 5 minutes for the configuration to take effect.

NOTICE

When you log in to a remote Windows server from another Windows server where 2FA is enabled, you need to manually add credentials on the latter. Otherwise, the login will fail.

To add credentials, choose **Start** > **Control Panel**, and click **User Accounts**. Click **Manage your credentials** and then click **Add a Windows credential**. Add the username and password of the remote server that you want to access.

----End

Copyright © Huawei Technologies Co., Ltd.

5 Server Management

5.1 Creating a Server Group

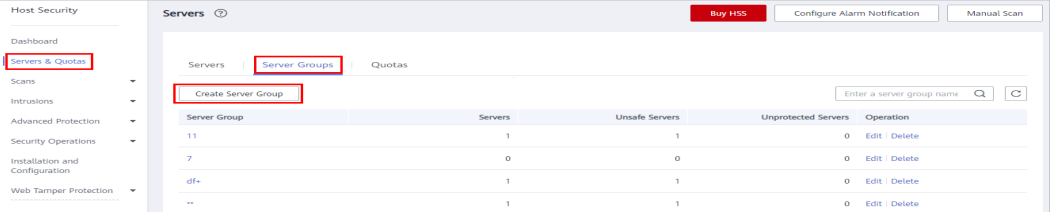
To manage servers by group, you can create a server group and add servers to it. You can check the numbers of servers, unsafe servers, and unprotected servers in a group.

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Servers**, and click the **Server Groups** tab. Click **Create Server Group**, as shown in **Figure 5-1**.

Figure 5-1 Accessing the Server Groups tab



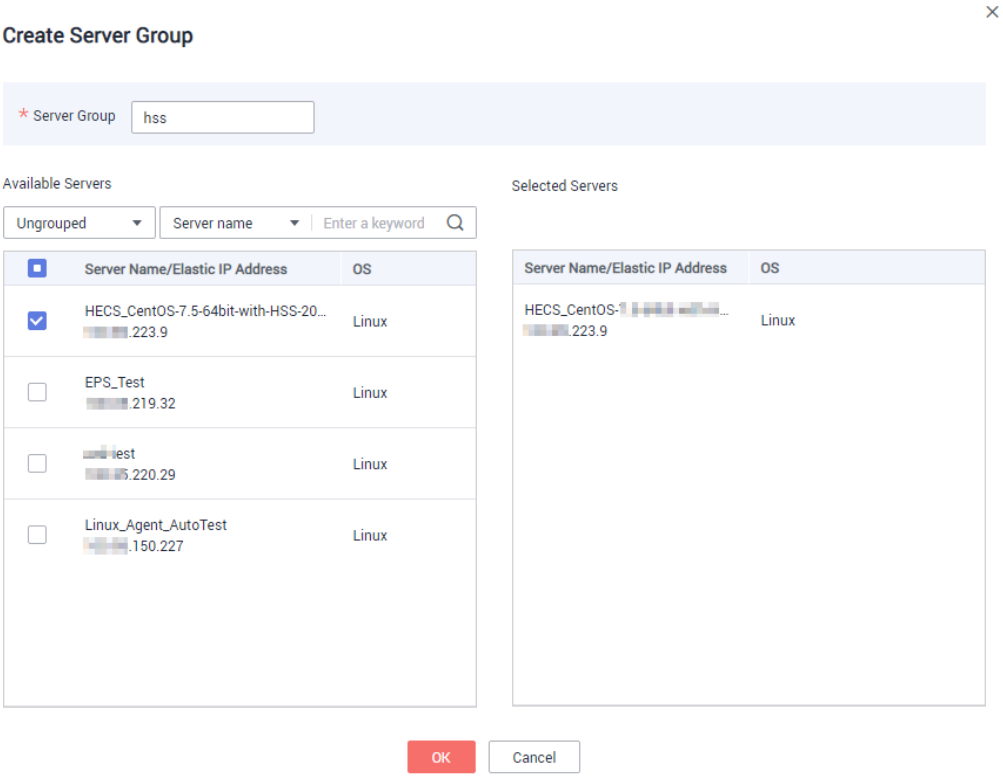
Step 4 In the **Create Server Group** dialog box, enter a server group name and select the servers to be added to the group, as shown in **Figure 5-2**.

NOTE

- A server group name must be unique, or the group will fail to be created.
- A name cannot contain spaces. It contains only letters, digits, underscores (_), hyphens (-), dots (.), asterisks (*), and plus signs (+). The length cannot exceed 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-2 Creating a server group



Step 5 Click **OK**.

----End

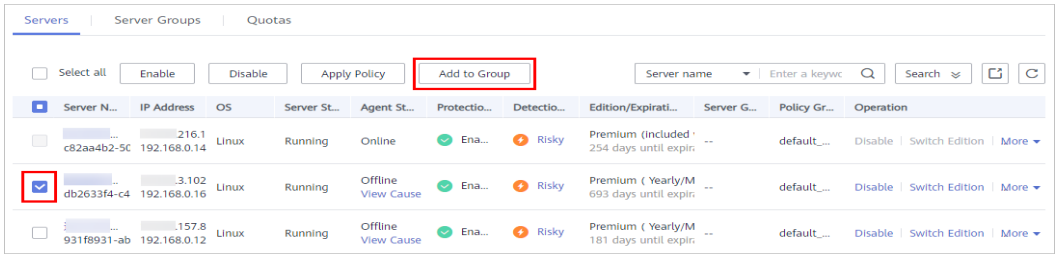
Adding Servers to Groups

You can add servers to an existing server group.

Step 1 Click the **Servers** tab.

Step 2 Select one or more servers and click **Add to Group**, as shown in **Figure 5-3**.

Figure 5-3 Adding servers to a group



NOTE

To add a server to a group, you can also locate the row where the server resides, click **More** in the **Operation** column, and choose **Add to Group**.

Copyright © Huawei Technologies Co., Ltd.

Step 3 In the displayed dialog box, select a server group and click **OK**.

NOTE

A server can be added to only one server group.

----End

Follow-Up Procedure

Editing a server group

Step 1 Locate the row where a server group resides and click **Edit** in the **Operation** column.

Step 2 In the displayed dialog box, add or remove servers in the group.

Step 3 Click **OK**.

----End

Viewing a server group

In the server group list, click the name of a server group to view the server status, agent status, protection status, and scan results of servers the group.

Deleting a server group

Locate the row where a server group resides and click **Delete** in the **Operation** column.

After the server group is deleted, the **Server Group** column of the servers that were in the group will be blank.

5.2 Applying a Policy

You can quickly configure and start server scans by using policy groups. Simply create a group, add policies to it, and apply this group to servers. The agents deployed on your servers will scan everything specified in the policies.

Precautions

- When you enable the enterprise edition, the default policy group of this edition (including weak password and website shell detection policies) takes effect for all your servers.
- When you enable the premium edition you separately purchased or included with the WTP edition, the default policy group of this edition takes effect.

  To create your own policy group, you can copy the default policy group and add or remove policies in the copy.

Accessing the Policies Page

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

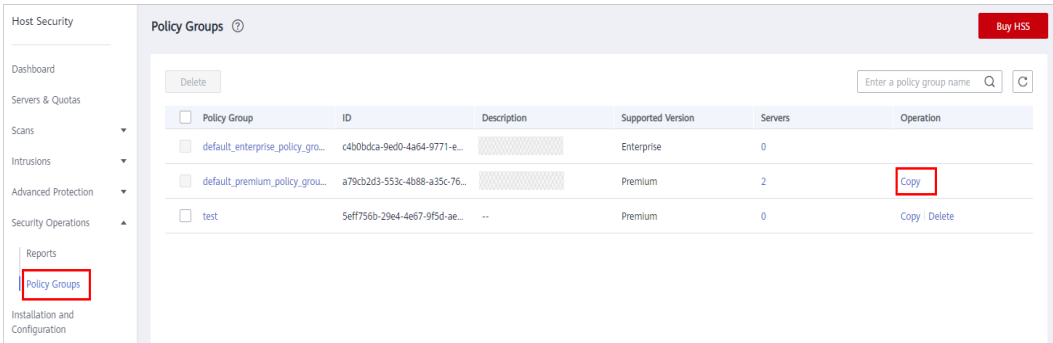
Step 3 In the navigation pane, choose **Security Operations** > **Policies**.

----End

Creating a Policy Group

Step 1 In the row where **default_premium_policy_group (default policy group of the premium edition)** resides, click **Copy** in the **Operation** column, as shown in **Figure 5-4**.

Figure 5-4 Copying a policy group

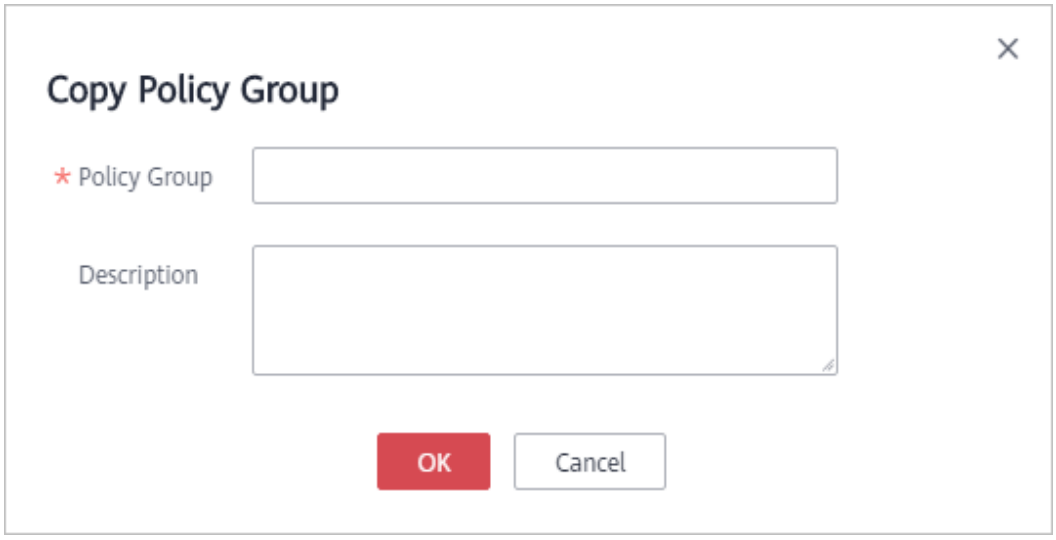


Step 2 In the dialog box displayed, enter a policy group name and description, and click **OK**, as shown in **Figure 5-5**.

NOTE

- The name of a policy group must be unique, or the group will fail to be created.
- The policy group name and its description can contain only letters, digits, underscores (_), hyphens (-), and spaces, and cannot start or end with a space.

Figure 5-5 Creating a policy group

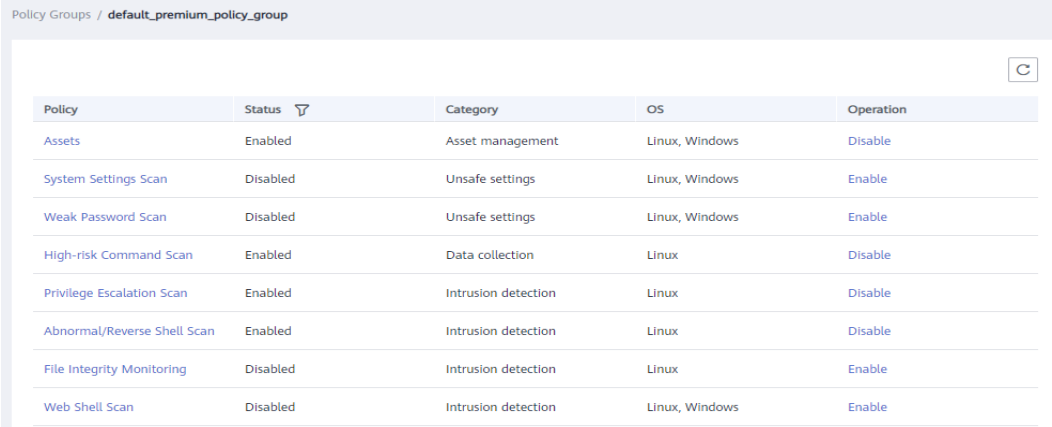


Step 3 Click **OK**.

Step 4 Click the name of the policy group you just created. The policies in the group will be displayed, as shown in **Figure 5-6**.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-6 Policies in a group



Policy	Status	Category	OS	Operation
Assets	Enabled	Asset management	Linux, Windows	Disable
System Settings Scan	Disabled	Unsafe settings	Linux, Windows	Enable
Weak Password Scan	Disabled	Unsafe settings	Linux, Windows	Enable
High-risk Command Scan	Enabled	Data collection	Linux	Disable
Privilege Escalation Scan	Enabled	Intrusion detection	Linux	Disable
Abnormal/Reverse Shell Scan	Enabled	Intrusion detection	Linux	Disable
File Integrity Monitoring	Disabled	Intrusion detection	Linux	Enable
Web Shell Scan	Disabled	Intrusion detection	Linux, Windows	Enable

Step 5 Click a policy name and modify its settings as required. For details, see **Modifying a Policy**.

Step 6 Enable or disable the policy by clicking the corresponding button in the **Operation** column.

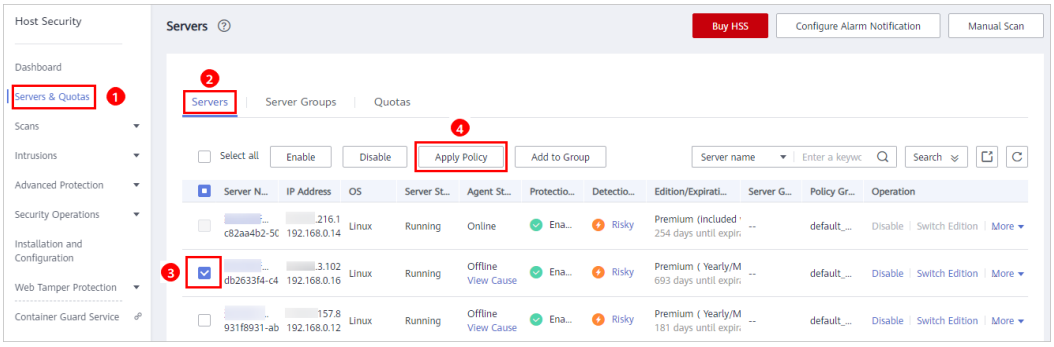
----End

Applying a Policy Group

Step 1 In the navigation pane, choose **Servers**. The **Servers** tab will be displayed.

Step 2 Select one or more servers and click **Apply Policy**, as shown in **Figure 5-7**.

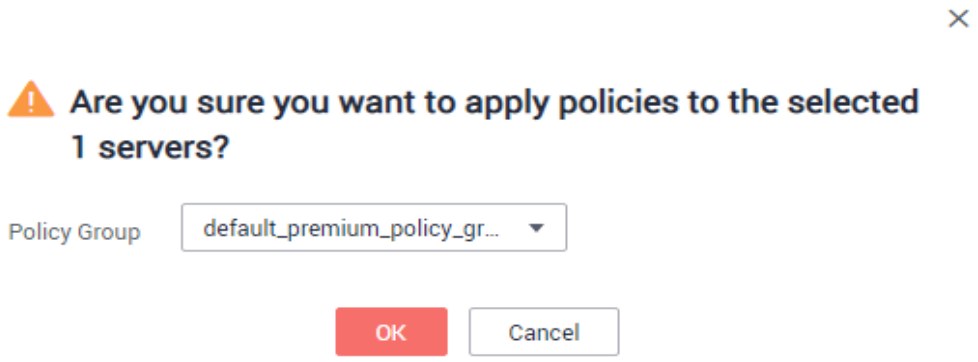
Figure 5-7 Applying policies



Step 3 In the dialog box that is displayed, select a policy group and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-8 Selecting a policy group



NOTE

- Old policies applied to a server will become invalid if you apply new policies to the server.
- Policies are applied to the servers within 1 minute.
- Policies applied to offline servers will not take effect until the servers are online.
- In a deployed policy group, you can enable, disable, or modify policies.
- A policy group that has been deployed cannot be deleted.

----End

5.3 Upgrading the Agent

You can upgrade Agent 1.0 to Agent 2.0 on the HSS platform. After the upgrade, your servers will be protected by HSS (New). You can check and manage the server protection status on the HSS (New) platform.

Prerequisites

- The **Agent Status** of the server must be **Online**.
- You are on the HSS (Old) console.

Upgrade Description

- Agent upgrade is free of charge.
- The upgrade does not affect services running on your cloud servers.
- After the upgrade, the billing stops on the old console and starts on the new console.
- After the upgrade, your servers will be protected by HSS (New).

NOTE

- Currently, HSS (New) is available in the following regions: CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.
- After switching to the new version, you can choose **Asset Management** > **Servers** and click **Back to Old Console** in the upper right corner to switch back to the old console.

Copyright © Huawei Technologies Co., Ltd.

- After the upgrade, you can enable enhanced ransomware prevention.
- After the upgrade, the new agent will be more secure, stable, and reliable.

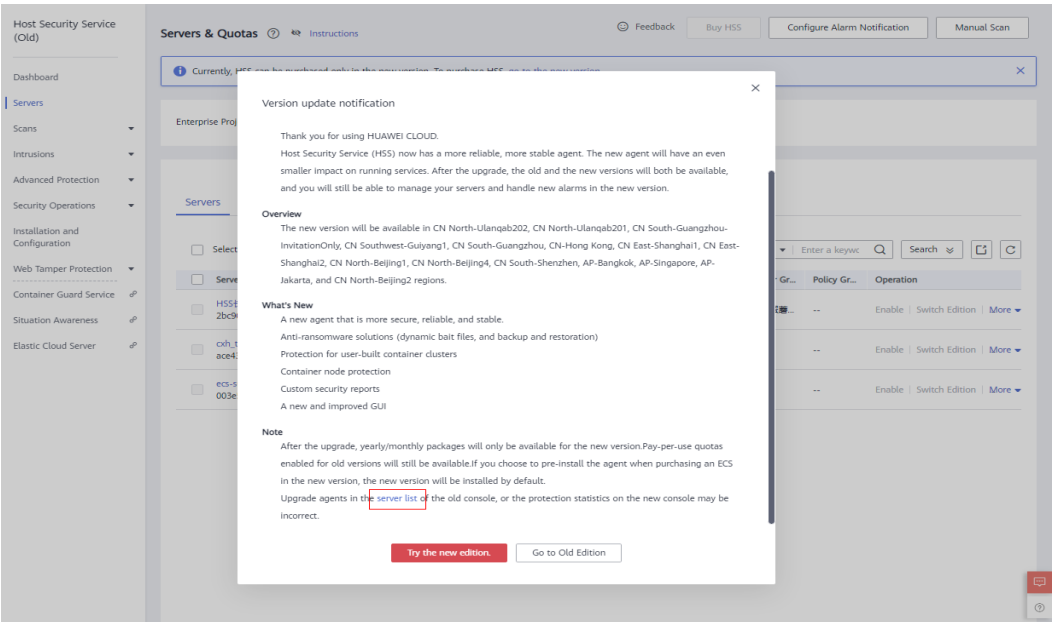
Procedure

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the upgrade notice that is displayed, click the **service list** link to go to the **Servers** tab of the HSS (Old) console.

Figure 5-9 Upgrading the agent



Step 4 Select servers and click **Upgrade to Agent 2.0**.

NOTE

Select one or more servers whose **Agent Status** is **Online**.

Step 5 In the dialog box, confirm the server information and click **OK**. The platform automatically performs the upgrade.

Step 6 Check the upgrade status by performing **5**.

The agent status can be **Upgrading**, **Upgraded**, or **Upgrade failed**.

----End

 Copyright © Huawei Technologies Co., Ltd.

6 Risk Prevention

6.1 Asset Management

HSS proactively checks open ports, processes, web directories, and auto-startup entries on your servers, and records changes on account and software information. For details about asset management, see **Asset Management**.

HSS lists all the assets on your servers and identifies risks in them in a timely manner.

HSS does not touch your assets. You need to manually eliminate the risks.

Check Interval

Account information and open ports are checked in real time. The open port detection result is updated every six hours.

Processes, web directories, software, and auto-start entries are checked in the early morning every day.

Viewing Asset Information

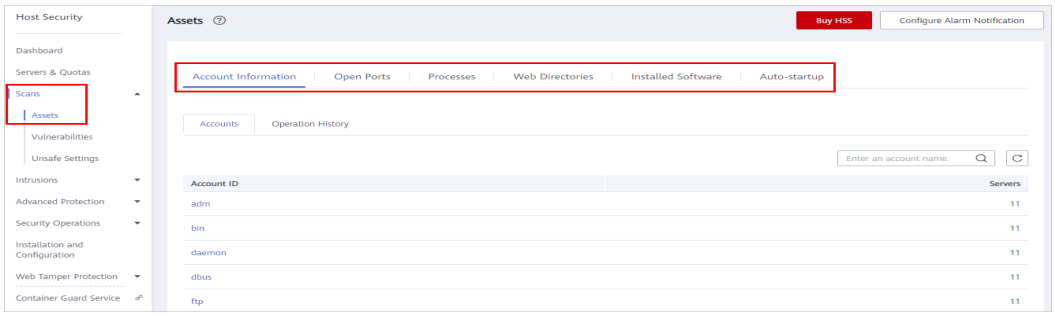
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Go to the **Assets** page. Click tabs on the page to view assets detected by HSS on your servers.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-1 Assets



----End

Managing Account Information

Operations made to accounts are recorded.

- The **Action** column records the operations. Its value can be **Create** (newly found in the latest check), **Delete** (found in earlier checks but missing in the latest check), and **Modify** (changes on account information, such as account names, administrator rights, and user groups, are detected).
- The **Time** column records the time when changes were detected, not the time when they were made.

You can check the information about and changes on all accounts here. If you find unnecessary or super-privileged accounts (such as **root**) that are not mandatory for services, delete them or modify their permissions to prevent exploits.

Checking Open Ports

You can manage all the open ports on your servers.

- Manually disabling high-risk ports

  If dangerous or unnecessary ports are found enabled, check whether they are mandatory for services, and disable them if they are not. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.

  It is recommended that you handle the ports with the **Dangerous** risk level promptly and handle the ports with the **Unknown** risk level based on the actual service conditions.
- Ignore risks: If a detected high-risk port is actually a normal port used for services, you can ignore it. The port will no longer be regarded risky or generate alarms.

Managing Processes

You can quickly check and terminate suspicious application processes on your servers.

If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.

 Copyright © Huawei Technologies Co., Ltd.

Managing Web Directories

You can check and delete risky web directories and terminate suspicious processes in a timely manner.

Managing Software

Operations made to software are recorded.

- **Action**: **Create** and **Delete**.
- The **Time** column records the time when changes were detected, not the time when they were made.

You can check the information about and changes on all software, upgrade software, and delete software that is unnecessary, suspicious, or in old version.

Managing Auto-start Entries

Trojans usually intrude servers by creating auto-started services, scheduled tasks, preloaded dynamic libraries, run registry keys, or startup folders. The auto-startup check function collects information about all auto-started items, including their names, types, and number of affected servers, making it easy for you to locate suspicious auto-started items.

You can check the servers, paths, file hashes, and last modification time of auto-started items to find and eliminate Trojans in a timely manner.

6.2 Vulnerability Management

6.2.1 Viewing Details of a Vulnerability

HSS detects Linux software vulnerabilities, Windows system vulnerabilities, and Web-CMS vulnerabilities.

On the **Vulnerabilities** page, you can view the basic information and status about vulnerabilities and handle them based on **Urgency**.

In the chart of top 5 servers, only the vulnerabilities of **High** urgency are displayed.

Detection Mechanisms

Table 6-1 Vulnerability detection mechanisms

Type	Mechanism
Linux vulnerabilities	HSS detects vulnerabilities in the system and software (such as SSH, OpenSSL, Apache, and MySQL) based on vulnerability libraries, reports the results to the management console, and generates alarms.

 Copyright © Huawei Technologies Co., Ltd.

Type	Mechanism
Windows vulnerabilities	HSS subscribes to Microsoft official updates, checks whether the patches on the server have been updated, pushes Microsoft official patches, reports the results to the management console, and generates vulnerability alarms.
Web-CMS vulnerabilities	HSS checks web directories and files for Web-CMS vulnerabilities, reports the results to the management console, and generates vulnerability alarms. The following types of software can be scanned: ● wordpress ● Joomla ● drupal ● discuz

NOTE

Vulnerabilities detected in the past 24 hours are displayed. The server name in a vulnerability notification is the name used when the vulnerability was detected, and may be different from the latest server name.

Real-time Vulnerability Database Update

HSS obtains official vulnerability information in real time and updates it to the vulnerability database.

Check Interval

HSS automatically performs a comprehensive scan in the early morning every day. You can export the scan report after the scan is complete.

Prerequisites

The enterprise, premium, or WTP edition of HSS has been enabled.

Fixing Linux or Windows Vulnerabilities

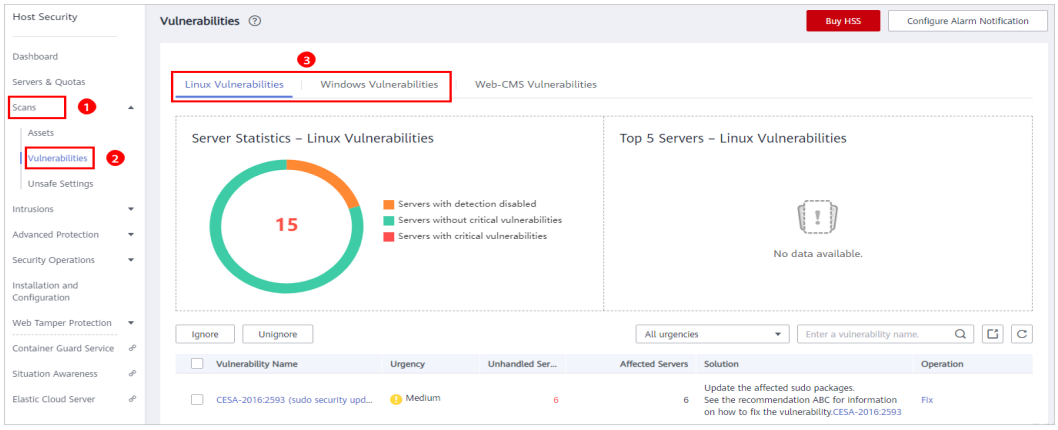
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Open the **Linux Vulnerabilities** or **Windows Vulnerabilities** tab.

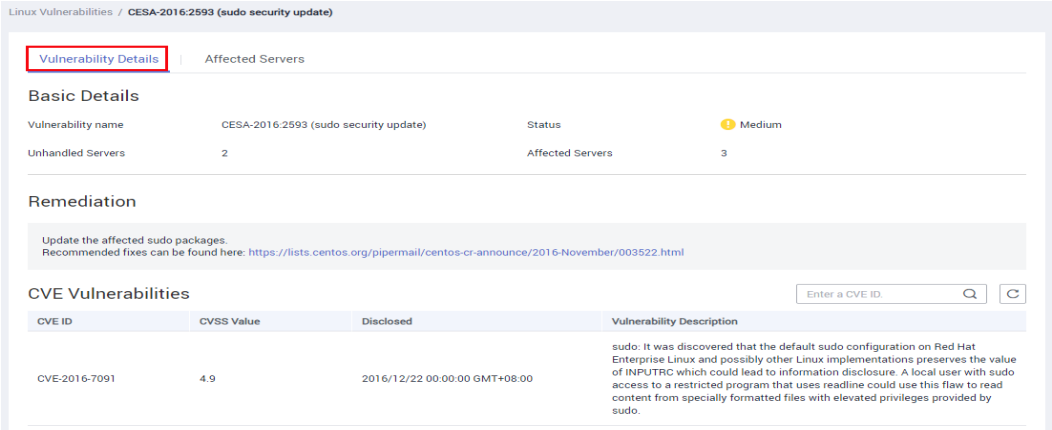
 Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Viewing Linux or Windows vulnerability scan results



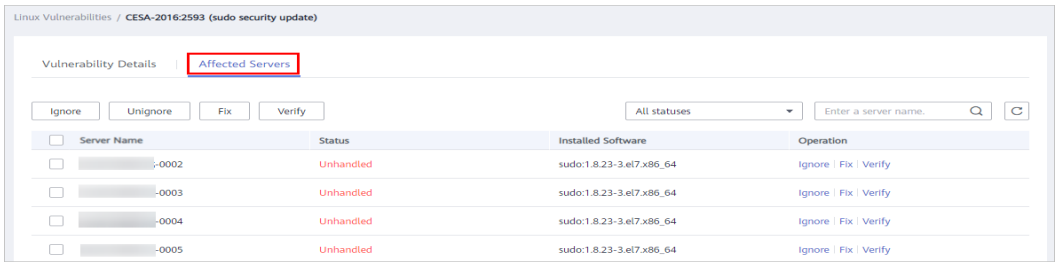
Step 4 Click a vulnerability name to view its basic information, solution, and CVE description.

Figure 6-3 Checking vulnerability details



Step 5 Check the servers affected by the vulnerability.

Figure 6-4 Checking affected servers



- To fix the vulnerability, click **Fix**.
- To ignore the vulnerability, click **Ignore**. HSS will no longer generate alarms for this vulnerability.
- After the vulnerability is fixed, you can click **Verify** to verify the fix.

  HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.

 Copyright © Huawei Technologies Co., Ltd.

If a vulnerability is still detected after you fix it, rectify the fault by referring to **Why the Alarms of Fixed Vulnerabilities Are Still Displayed?**

If a vulnerability fails to be rectified, click **View Cause** to check the details.

----End

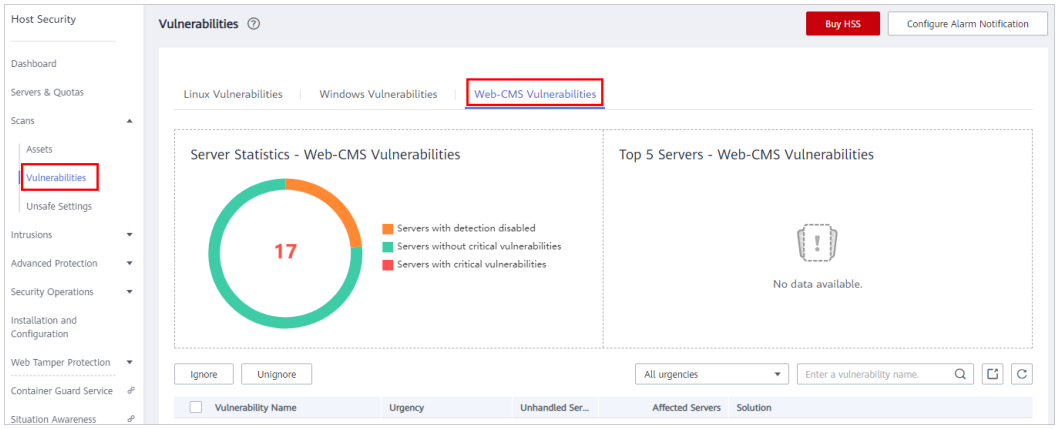
Fixing Web-CMS Vulnerabilities

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Open the **Web-CMS Vulnerabilities** tab.

Figure 6-5 Viewing Web-CMS vulnerability detection results



Step 4 Click the vulnerability name to view its details and affected servers.

- No **Fix** options are provided in the **Operation** column. You need to manually fix the vulnerabilities based on the suggestions provided.
- After the vulnerability is fixed, manually verify the result. HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.
- To ignore the vulnerability, click **Ignore**. HSS will no longer generate alarms for this vulnerability.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-6 Vulnerability details

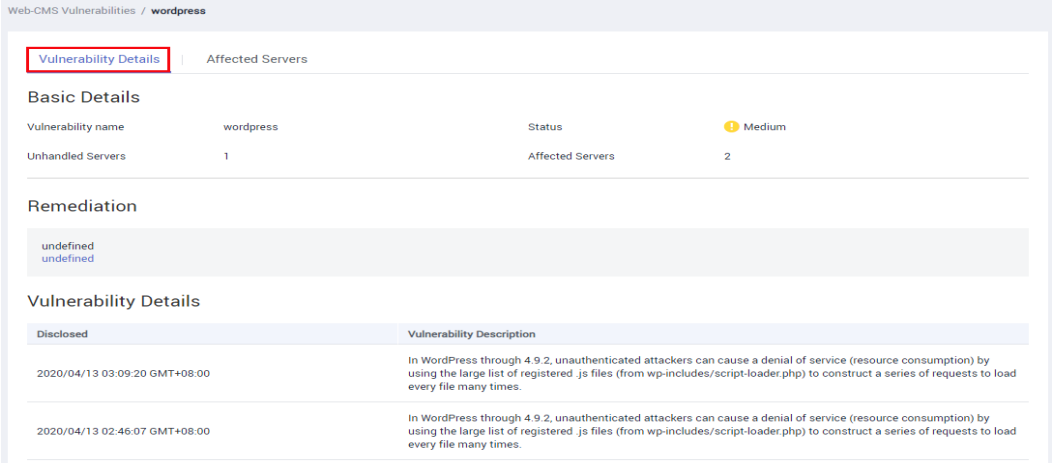
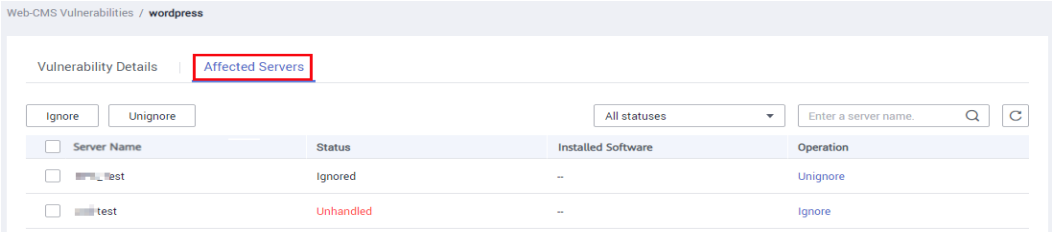


Figure 6-7 Affected servers



----End

Exporting a Vulnerability Report

In the upper right corner of the vulnerability list, click  to export the vulnerability report.

NOTICE

- A maximum of 5000 vulnerability data records can be exported from HSS.

For example, HSS detected two vulnerabilities P1 and P2. P1 exists on N servers and P2 exists on M servers. N+M vulnerability records will be exported.

- The report contains the vulnerability information about all the scanned servers.
- HSS automatically performs a comprehensive scan in the early morning every day. After the scan is complete, you can download the vulnerability report. To perform a manual scan, **upgrade to the HSS (New) version**. You can export the scan report immediately after the scan is complete.

6.2.2 Fixing Vulnerabilities and Verifying the Result

- Linux or Windows vulnerabilities

  You can select servers and click **Fix** to let HSS fix the vulnerabilities for you, or manually fix them based on the suggestions provided.

Copyright © Huawei Technologies Co., Ltd.

Then, you can use the verification function to quickly check whether the vulnerability has been fixed.

NOTICE

To fix Windows vulnerabilities, you need to connect to the Internet.

- Web-CMS vulnerabilities

  Manually fix them based on the suggestions provided on the page.

Precautions

- Vulnerability fixing operations cannot be rolled back. If a vulnerability fails to be fixed, services will probably be interrupted, and incompatibility issues will probably occur in middleware or upper layer applications. To avoid unrecoverable errors, you are advised to use Cloud Server Backup Service (CSBS) to back up your servers. For details, see **Creating a CSBS Backup**. Then, use idle servers to simulate the production environment and test-fix the vulnerability. If the test-fix succeeds, fix the vulnerability on servers running in the production environment.
- Servers need to access the Internet and use external image sources to fix vulnerabilities. If your servers cannot access the Internet, or the external image sources cannot provide stable services, you can use the image source provided by HUAWEI CLOUD to fix vulnerabilities.

  Before fixing vulnerabilities online, configure the HUAWEI CLOUD image sources that match your server OSs. For details, see **Image Source Management**.
- After a vulnerability is fixed, you are advised to restart the server to refresh its status. Otherwise, the vulnerability information may still be pushed to you.

Urgency

- **High**: This vulnerability must be fixed as soon as possible. Attackers may exploit this vulnerability to damage the server.
- **Medium**: You are advised to fix the vulnerability to enhance your server security.
- **Safe for now**: This vulnerability has a small threat to server security. You can choose to fix or ignore it.

Vulnerability Display

- Vulnerabilities that failed to be fixed or have not been handled are always displayed in the vulnerability list.
- Fixed vulnerabilities will remain in the list within 30 days after it was fixed.

Fixing Vulnerabilities in One Click

You can fix vulnerabilities in Linux or Windows OS in one click on the console.

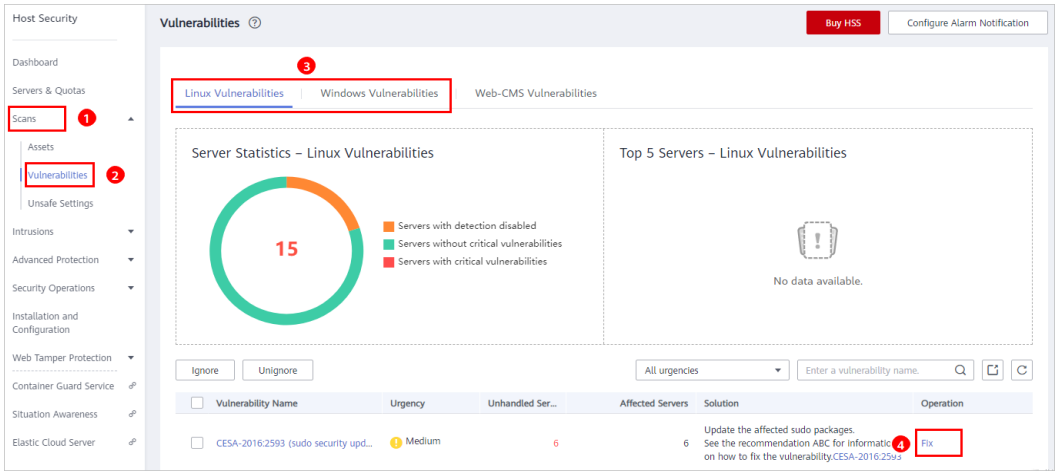
Step 1 **Log in to the management console.**

 Copyright © Huawei Technologies Co., Ltd.

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

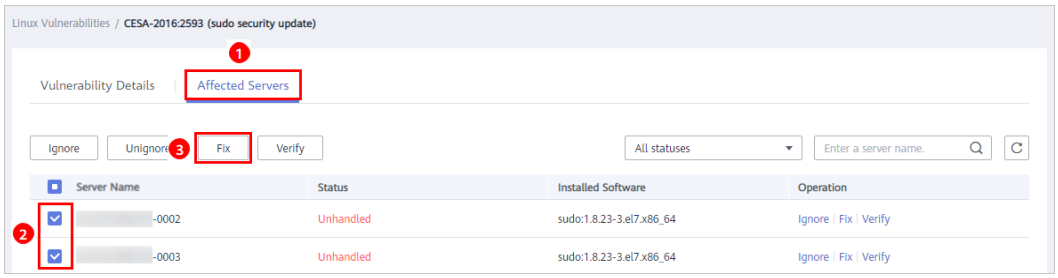
Step 3 On the **Vulnerabilities** page, click **Fix**. The **Affected Servers** tab is displayed, as shown in **Figure 6-8**.

Figure 6-8 Fixing vulnerabilities



Step 4 Select the affected servers and click **Fix**.

Figure 6-9 One-click vulnerability fix



Step 5 In the dialog box that is displayed, select **I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.**

Step 6 Click **OK** to fix the vulnerability in one-click mode. The vulnerability status will change to **Fixing**.

If a vulnerability is fixed, its status will change to **Fixed**. If it fails to be fixed, its status will change to **Failed**.

NOTE

- Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.
- After the Windows OS is restarted, you need to confirm the restart on the console.

----End

 Copyright © Huawei Technologies Co., Ltd.

Manually Fixing Software Vulnerabilities

Fix the detected vulnerability based on the fix suggestions in the **Solution** column. For details about the vulnerability fix commands, see **Table 6-2**.

- Fix the vulnerabilities in sequence based on the suggestions.
- If multiple software packages on the same server have the same vulnerability, you only need to fix the vulnerability once.

NOTE

Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

Table 6-2 Vulnerability fix commands

OS	Command
CentOS/Fedora/EulerOS/Red Hat/Oracle	**yum update** *Software_name*
Debian/Ubuntu	**apt-get update && apt-get install** *Software_name* **--only-upgrade**
Gentoo/SUSE	See the vulnerability fix suggestions for details.

Vulnerability fixing may affect service stability. You are advised to use either of the following methods to avoid such impact:

Method 1: Create a VM to fix the vulnerability.

1. Create an image for the ECS host whose vulnerability needs to be fixed. For details, see **Creating a Full-ECS Image from an ECS**..
2. Use the image to create a new ECS host. For details, see **Creating an ECS from an Image**..
3. Fix the vulnerability on the new ECS and verify the result.
4. Switch services over to the new ECS and verify they are stably running.
5. Release the original ECS. If a fault occurs after the service switchover and cannot be rectified, you can switch services back to the original ECS.

Method 2: Fix the vulnerability on the target server.

1. Create a backup for the ECS to be fixed. For details, see **Creating a CSBS Backup**.
2. Fix vulnerabilities on the current server.
3. If services become unavailable after the vulnerability is fixed and cannot be recovered in a timely manner, use the backup to restore the server. For details, see **Using Backups to Restore Servers**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Use method 1 if you are fixing a vulnerability for the first time and cannot estimate impact on services. You are advised to choose the pay-per-use billing mode for the newly created ECS. After the service switchover, you can change the billing mode to yearly/monthly. In this way, you can release the ECS at any time to save costs if the vulnerability fails to be fixed.
- Use method 2 if you have fixed the vulnerability on similar servers before.

Ignoring Vulnerabilities

Some vulnerabilities are risky only in specific conditions. For example, if a vulnerability can be exploited only through an open port, but the target server does not open any ports, the vulnerability will not harm the server. Such vulnerabilities can be ignored.

HSS will not generate alarms for ignored vulnerabilities.

Verifying Vulnerability Fix

After a vulnerability is fixed, you are advised to verify it immediately.

Manual verification

- Click **Verify** on the vulnerability details page.
- Ensure the software has been upgraded to the latest version. The following table provides the commands to check the software upgrade result.

Table 6-3 Verification commands

OS	Verification Command
CentOS/Fedora/EulerOS/Red Hat/Oracle	rpm -qa | grep *Software_name*
Debian/Ubuntu	dpkg -l | grep *Software_name*
Gentoo	emerge --search *Software_name*
SUSE	zypper search -dC --match-words *Software_name*

- **Manually check for vulnerabilities** and view the vulnerability fixing results.

Automatic verification

HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.

6.3 Baseline Inspection

6.3.1 Checking for Unsafe Settings

HSS checks your software for weak password complexity policies and other unsafe settings, and provides **suggestions** for fixing detected risks. For details about baseline, see **Baseline Inspection**.

Check Interval

- HSS automatically performs a comprehensive check in the early morning every day.
- To manually start a scan, click **Manual Scan** in the upper right corner of the **Servers** page.

  HSS will scan your servers for software information, Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, web shells, password risks, and unsafe settings configuration.

  All these items are concurrently checked and the total scan duration is less than 30 minutes.
- To view the scan details of a server, click its scan result in the **Detection Result** column on the **Servers and Quotas** page.

  You can also scan for password risks or unsafe configurations alone. On the **Unsafe Settings** tab of the result page, click the **Password Risks** or **Unsafe Configurations** subtab and click **Scan**. The scan takes less than 30 minutes.

Alarm Policies

HSS checks your servers for weak passwords and unsafe software settings, and generates alarms if it finds any of them.

NOTE

You can enable alarm notifications on the **Installation and Configuration** page of the HSS console. For details, see **Enabling the Basic/Enterprise/Premium Edition**.

Check Items

Table 6-4 Check items

Item	Description
Common weak passwords	Weak passwords defined in the common weak password library Common weak passwords of MySQL, FTP, and system accounts
Password complexity policies	Password complexity policies on system accounts

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Unsafe configurations	Unsafe configurations found based on security best practices and Center for Internet Security (CIS) standards Unsafe configurations in Tomcat, SSH, Nginx, Redis, Apache2, MySQL5, MongoDB, Windows, vsftp, and CentOS.

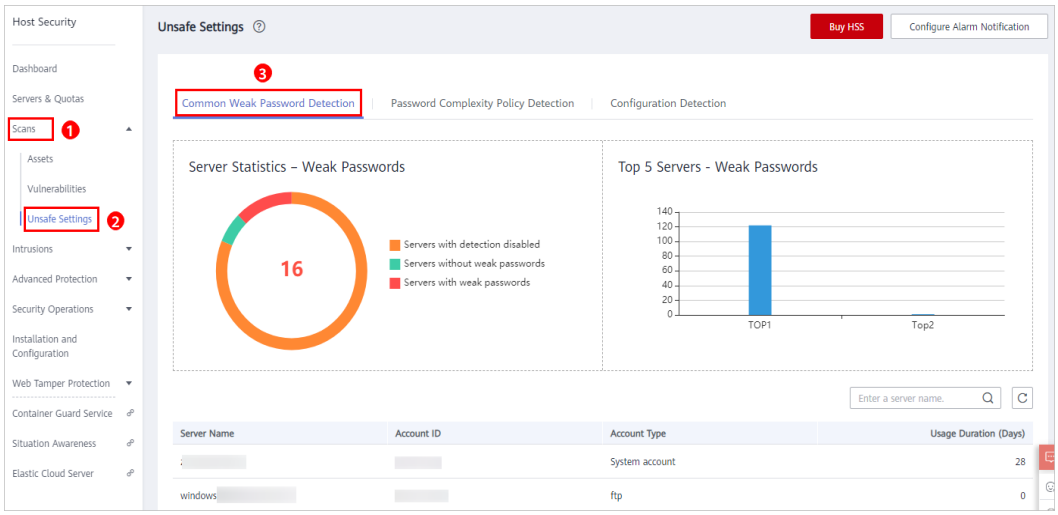
Procedure

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Scans** > **Unsafe Settings** and check detected unsafe settings.

Figure 6-10 Unsafe settings



----End

Exporting a Check Report

On the upper right corner of the table on the **Configuration Detection** tab, click  to download reports.

NOTE

The detection result of a single server cannot be separately exported.

6.3.2 Suggestions on Fixing Unsafe Settings

This topic provides suggestions on how to fix unsafe settings found by HSS.

 Copyright © Huawei Technologies Co., Ltd.

Weak Passwords

- To enhance server security, you are advised to modify the accounts with weak passwords for logging in to the system in a timely manner, such as SSH accounts.
- To protect internal data of your server, you are advised to modify software accounts that use weak passwords, such as MySQL accounts and FTP accounts.

Verification: After you modified weak passwords, **perform a manual scan** again. If you do not perform manual verification, HSS will automatically check the settings the next day in the early morning.

Modifying the Password Complexity Policy

- To monitor the password complexity policy on a Linux server, install the Pluggable Authentication Modules (PAM) on the server. For details, see **How Do I Install a PAM in a Linux OS?**
- For details about how to modify the password complexity policy on a Linux host, see **Setting a Password Complexity Policy**.
- For details about how to modify the password complexity policy on a Windows host, see **Setting a Password Complexity Policy**.

Verification: After you modified the password complexity policy, **perform a manual scan** again. If you do not perform manual verification, HSS will automatically check the settings the next day in the early morning.

Unsafe Configurations

Insecure configurations of key applications will probably be exploited by hackers to intrude servers. Such configurations include insecure encryption algorithms used by SSH and Tomcat startup with root permissions.

HSS can detect unsafe configurations provide detailed suggestions. You can check, fix, or ignore a risky item.

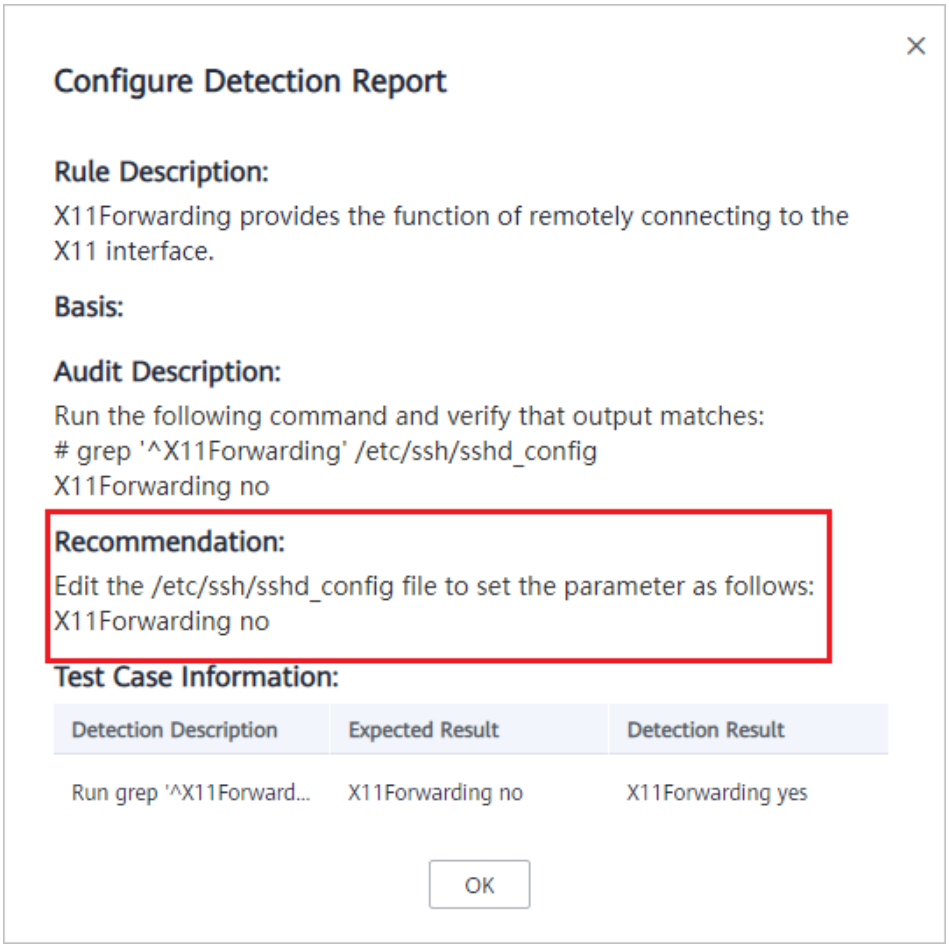
- Modifying unsafe configuration items

  You can confirm the detection result based on details under **Audit Description** and fix settings as instructed in **Recommendation**.

  You are advised to fix the configurations with high severity immediately and repair those with medium or low severity based on service requirements.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-11 Detection report



- Ignoring trusted configuration items

  Select a detection rule and click **Ignore** in the **Operation** column to ignore it. To ignore multiple detection rules, select them and click the **Ignore** button above the list to batch ignore them.

  To unignore an ignored detection rule, click **Unignore** in the **Operation** column. To unignore multiple ignored detection rules, select rules and click **Unignore** in the upper left corner above the detection rule list.

Verification: After you modified configuration items, **perform a manual scan** again. If you do not perform manual verification, HSS will automatically check the settings the next day in the early morning.

 Copyright © Huawei Technologies Co., Ltd.

7 Intrusion Detection

7.1 Alarm Events

HSS generates alarms on 13 types of intrusion events, including brute-force attacks, abnormal process behavior, web shells, abnormal logins, and malicious processes. You can learn all these events on the HSS console and eliminates security risks in your assets in a timely manner.

Alarm Events

NOTE

The basic edition provides only part of the security scan capabilities. This edition does not provide protection capabilities, nor does it provide support for DJCP MLPS certification.

To protect your ECSs or pass the DJCP MLPS certification, purchase the enterprise edition or a higher edition (premium edition or Web Tamper Protection edition).

 Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Brute-force attack	If hackers log in to your servers through brute-force attacks, they can obtain the control permissions of the servers and perform malicious operations, such as steal user data; implant ransomware, miners, or Trojans; encrypt data; or use your servers as zombies to perform DDoS attacks. Detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts. ● If the number of brute-force attacks (consecutive incorrect password attempts) from an IP address reaches 5 within 30 seconds, the IP address will be blocked. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. ● You can check whether the IP address is trustworthy based on its attack type and how many times it has been blocked. You can manually unblock the IP addresses you trust.	√	√	√	√
Abnormal login	Detect abnormal login behavior, such as remote login and brute-force attacks. If abnormal logins are reported, your servers may have been intruded by hackers. ● Check and handle remote logins. You can check the blocked login IP addresses, and who used them to log in to which server at what time. If a user's login location is not any common login location you set, an alarm will be triggered. ● Trigger an alarm if a user logs in by a brute-force attack.	√	√	√	√

Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Malicious program (cloud scan)	Malicious programs include Trojans and web shells implanted by hackers to steal your data or control your servers. For example, hackers will probably use your servers as miners or DDoS zombies. This occupies a large number of CPU and network resources, affecting service stability. Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants, and kill them in one click. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing. **NOTE** HSS can detect only running malicious programs.	×	√ (Isolate and kill)	√ (Isolate and kill)	√ (Isolate and kill)
Abnormal process behavior	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: ● Abnormal CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections	×	√	√	√

Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Critical file change	If hackers intrude into your system, they will probably tamper with important system files to forge identities or prepare for further attacks. ● Check alarms about modifications on key files (such as **ls**, **ps**, **login**, and **top**). For details about the monitored paths, see **Monitored Important File Paths**. ● Key file change information includes the paths of modified files, the last modification time, and names of the servers storing configuration files. ● You can add fingerprint libraries of critical files, so that HSS can better collect critical file information and detect exceptions. HSS only checks whether directories or files have been modified, not whether they are modified manually or by a process.	×	√	√	√
Web shell	A web shell is a command execution environment in the form of web page files, such as PHP and JSP files. After hacking a website, a hacker usually puts a web shell among normal web page files in the web directory of a website server, and then accesses the web shell through a browser to control the server. Check whether the files (often PHP and JSP files) in your web directories are web shells. ● Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. ● You can use the manual detection function to detect web shells on servers.	×	√	√	√

Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Reverse shell	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. You can configure the reverse shell detection rule on the **Policies** page. HSS will check for suspicious or remotely executed commands.	×	×	√	√
Abnormal shell	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. You can configure the reverse shell detection rule on the **Policies** page. HSS will check for suspicious or remotely executed commands.	×	×	√	√
High-risk command execution	You can configure what commands will trigger alarms in the **High-risk Command Scan** rule on the **Policies** page. HSS checks executed commands in real time and generates alarms if high-risk commands are detected.	×	×	√	√
Auto-startup check	Trojans usually intrude servers by creating auto-started services, scheduled tasks, or preloaded dynamic libraries. The auto-startup check function collects information about all auto-started items, including their names, types, and number of affected servers. HSS checks and lists auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders.	×	×	√	√
Unsafe account	Hackers can probably crack unsafe accounts on your servers and control the servers. HSS checks suspicious hidden accounts and cloned accounts and generates alarms on them.	×	√	√	√

Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Privilege escalation	After hackers intrude servers, they will try exploiting vulnerabilities to grant themselves the root permissions or add permissions for files. In this way, they can illegally create system accounts, modify account permissions, and tamper with files. HSS detects privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities ● File privilege escalation	×	×	√	√
Rootkit	HSS detects suspicious rootkit installation in a timely manner by checking: ● Rootkits based on file signatures ● Hidden files, ports, and processes	×	×	√	√

Monitored Important File Paths

Type	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/netstat /bin/login /bin/find /bin/lsmod /bin/pidof /bin/lsof /bin/ss

Copyright © Huawei Technologies Co., Ltd.

Type	Linux
usr	/usr/bin/ls /usr/bin/ps /usr/sbin/ps /usr/bin/bash /usr/bin/netstat /usr/sbin/netstat /usr/sbin/rsyslogd /usr/sbin/ifconfig /usr/bin/login /usr/bin/find /usr/sbin/lsmod /usr/sbin/pidof /usr/bin/lsof /usr/sbin/lsof /usr/sbin/tcpd /usr/bin/passwd /usr/bin/top /usr/bin/du /usr/bin/chfn /usr/bin/chsh /usr/bin/killall /usr/bin/ss /usr/sbin/ss /usr/bin/ssh /usr/bin/scp
sbin	/sbin/syslog-ng /sbin/rsyslogd /sbin/ifconfig /sbin/lsmod /sbin/pidof

7.2 Checking and Handling Intrusion Events

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of servers with alarms, handled alarms, unhandled alarms, blocked IP addresses, and isolated files.

The **Events** page displays the alarm events generated in the last 30 days.

The status of a handled event changes from **Unhandled** to **Handled**.

NOTE

An alarm indicates that an attack was detected. It does not mean your cloud servers have been intruded.

If you receive an alarm, handle it and take countermeasures in a timely manner.

Constraints and Limitations

- To skip the checks on high-risk command execution, privilege escalation, reverse shells, abnormal shells, or web shells, manually disable the corresponding policies in the policy groups on the **Policies** page. HSS will not check the servers associated with disabled policies. For details, see **Checking or Creating a Policy Group**.
- Other detection items cannot be manually disabled.

Checking Alarm Events

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Intrusions** > **Events**, as shown in **Figure 7-1**.

Figure 7-1 Events page

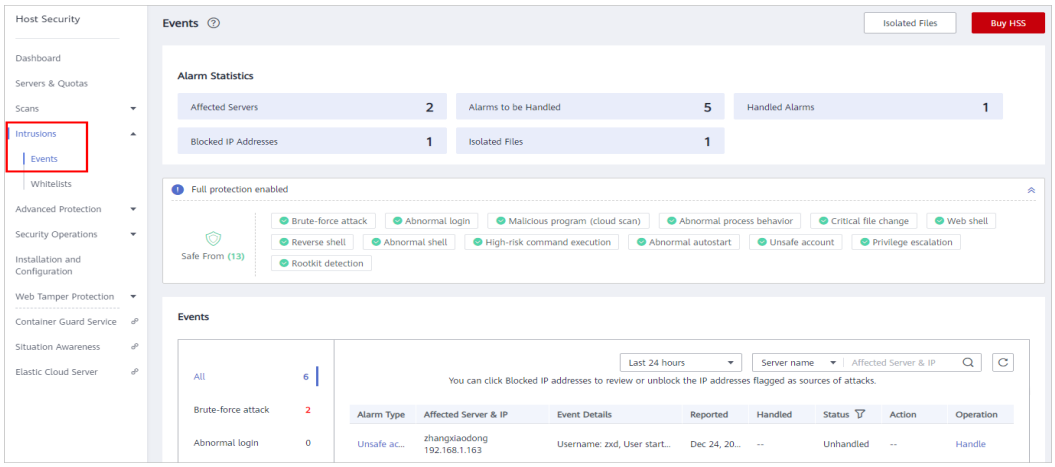


Table 7-1 Alarm events

Alarm Event	Description
Affected Servers	Number of servers for which alarms are generated.
Alarms to be Handled	Number of alarms to be handled. By default, all unhandled alarms are displayed on the **Events** page. For more information, see **Handling Alarm Events**.

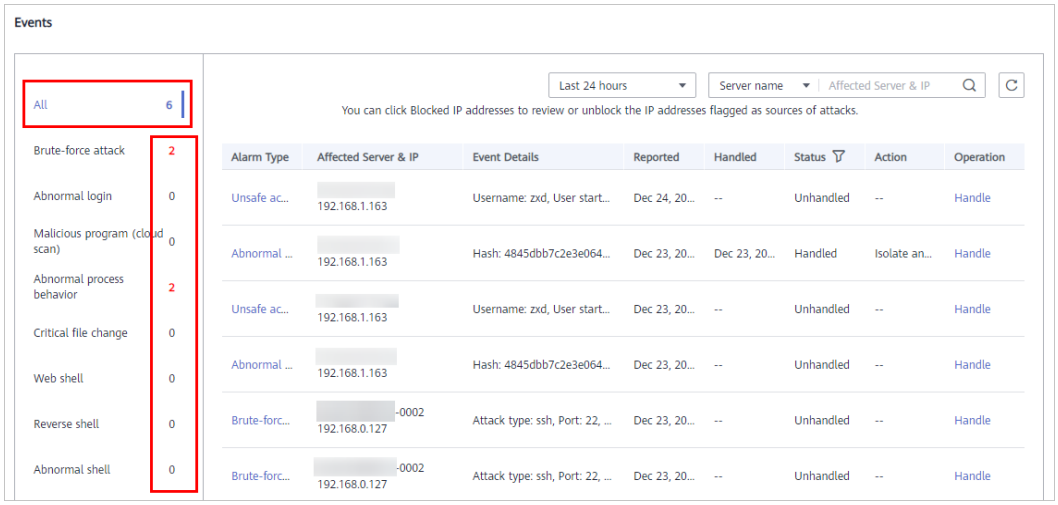
 Copyright © Huawei Technologies Co., Ltd.

Alarm Event	Description
Handled Alarms	Number of handled alarms.
Blocked IP Addresses	Number of blocked IP addresses. You can click the number to check blocked IP address list. The blocked IP address list displays the server names, blocked IP addresses, attack types, number of blocked attacks, the first and last time the IP addresses are blocked, block durations, and status. If a valid IP address is blocked by mistake (for example, after O&M personnel enter incorrect passwords for multiple times), you can manually unblock it. If a server is frequently attacked, you are advised to fix its vulnerabilities in a timely manner and eliminate risks. **NOTICE** After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address.
Isolated Files	HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Events** page. You can click **Isolated Files** on the upper right corner to check them. You can recover isolated files. For details, see **Managing Isolated Files**.

Step 4 Click an alarm event in the list to view the affected servers and occurrence time of the event, as shown in **Figure 7-2**. The following information is displayed:

- Total number of alarms
- Number of each type of alarms

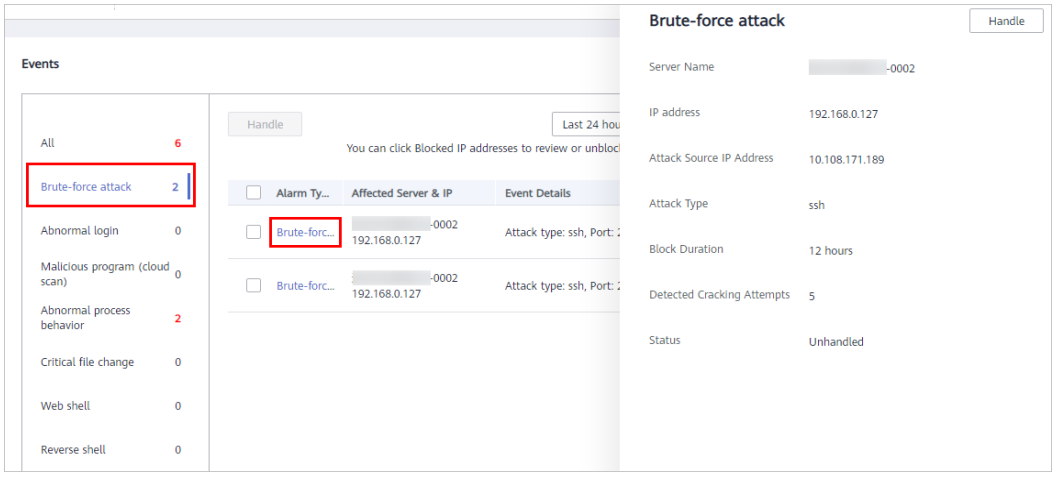
Figure 7-2 Alarm event statistics



Step 5 Click an alarm name to view its details, as shown in **Figure 7-3**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-3 Alarm details



----End

Handling Alarm Events

This section describes how you should handle alarm events to ensure server security.

NOTE

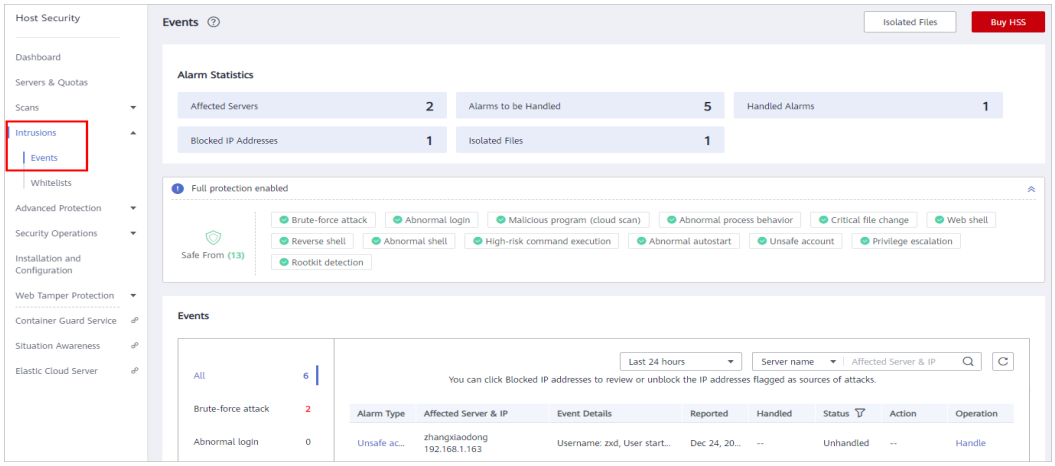
Do not fully rely on alarms to defend against attacks, because not every issue can be detected in a timely manner. You are advised to take more measures to prevent threats, such as checking for and fixing vulnerabilities and unsafe settings.

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Intrusions** > **Events**.

Figure 7-4 Events page



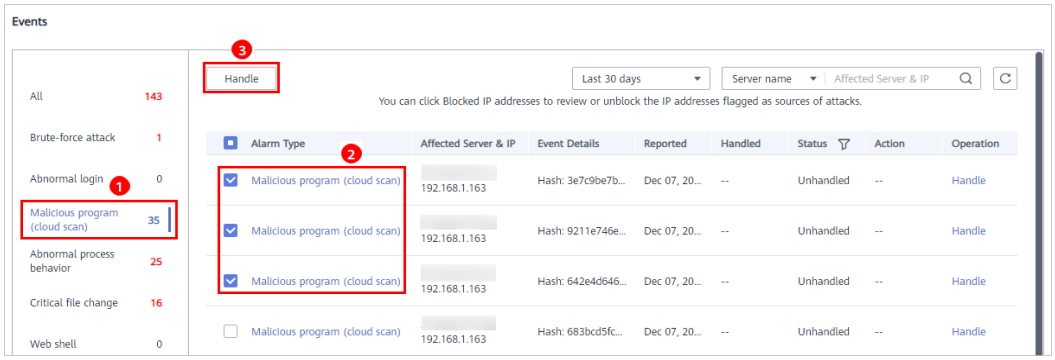
Step 4 Click an event type, select events, and click **Handle**, as shown in **Figure 7-5**. **Table 7-2** describes the processing methods you can choose from.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also click **Handle** in the row where an alarm resides.

Figure 7-5 Handling alarm events



Alarm events are displayed on the **Events** page. Here you can check up to 30 days of historical events.

Check and handle alarm events as needed. The status of a handled event changes from **Unhandled** to **Handled**. HSS will no longer collect its statistics or display them on the **Dashboard** page.

Table 7-2 Event handling methods

Method	Description
Ignore	Ignore the current alarm. Any new alarms of the same type will still be reported by HSS.
Isolate and kill	If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check the files. For details, see **Managing Isolated Files**. The following types of alarm events support online isolation and killing: ● Malicious program (cloud scan) ● Abnormal process behavior **NOTE** When a program is isolated and killed, the process of the program is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious programs (if any).
Mark as handled	Mark the event as handled. You can add remarks for the event to record more details.

Copyright © Huawei Technologies Co., Ltd.

Method	Description
Add to whitelist	Add false alarmed items of the **Brute-force attack** and **Abnormal login** types to the login whitelist. HSS will no longer report alarm on the whitelisted items.
Add to alarm whitelist	Add false alarmed items of the following types to the login whitelist. HSS will no longer report alarm on the whitelisted items. ● Reverse shell ● Web shell ● Abnormal process behavior ● Process privilege escalation ● File privilege escalation ● High-risk command ● Malicious program

----End

 Copyright © Huawei Technologies Co., Ltd.

Handling Suggestions

Alarm Name	Parameter	Suggestion
Brute-force attack	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Attack Source IP Address**: attacking server IP address • **Attack Type**: type of the blocked attack. It can be **mysql**, **mssql**, **vsftp**, **filezilla**, **serv-u**, **ssh**, or **rdp**. • **Detected Cracking Attempts**: number of account cracking attempts detected • **Status**: Event status. It can be **Handled** or **Unhandled**.	**Pay special attention to such events.** If you receive a brute-force attack alarm, detected events will probably be but are not limited to: • The system uses weak passwords and is under brute-force attacks. • Attackers correctly guess the password and log in after several failed attempts (before their login IP addresses are blocked). You are advised to check whether the alarmed login IP address is valid. • If the source IP address is valid, ignore the alarms and manually unblock the IP addresses. Alternatively, whitelist the alarmed IP address. This IP address will no longer trigger alarms. • If the source login IP address are unknown, your servers may have been intruded by hackers. 1. You are advised to mark the event as **Handled**. 2. Immediately log in to the intruded account and set a strong password. 3. Check all the accounts and delete suspicious accounts to prevent attackers from creating new accounts or changing account permissions. 4. Check for malicious programs on servers. Then, log in to the servers where the malicious programs are running and stop them immediately.

Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Parameter	Suggestion
Abnormal login	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Attack Type**: type of the attack. It can be **mysql**, **mssql**, **vsftp**, **filezilla**, **serv-u**, **ssh**, or **rdp**. • **Port**: attacked port • **Server**: attacking server IP address • **Username**: abnormal login account • **Status**: Event status. It can be **Handled** or **Unhandled**.	If an abnormal login is detected, you are advised to immediately check whether the source IP address is valid. • If it is valid, you can ignore this event. If the login location is valid, you can add the location to the list of common login locations. • If it is invalid or unknown, your servers have been intruded. In this case, you are advised to mark the event as **Handled**, immediately change the account password, and scan the entire system for risks to prevent further damage.

 Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Parameter	Suggestion
Malicious program (cloud scan)	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Program Path**: malicious program path • **Hash**: hash value • **File Permission**: permissions for the file • **User**: user who runs the program • **Program Started**: time when the program was started • **Status**: Event status. It can be **Handled** or **Unhandled**.	Common methods to handle the event are as follows: • If the programs are normal, ignore the event or whitelist the program. The programs will no longer trigger such events. • If the programs are unknown or malicious, you are advised to immediately kill them and isolate their source files. – You can isolate and kill detected or suspicious programs in one click. Alternatively, you can mark the event as **Handled**, immediately log in and stop the program, and scan the entire system for risks to prevent further damage. – HSS can isolate and kill malicious programs, including common ransomware, DDoS viruses, and Trojans. You are advised to enable this function to harden server security. For details, see **Isolating and Killing Malicious Programs**. • If the programs are harmless or mandatory for service operation, you can cancel isolation and restore the program source files.

Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Parameter	Suggestion
Abnormal process behavior	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Program Path**: suspicious program path • **File Permission**: permissions for the file • **PID**: process ID • **Command Line**: command line used to start the abnormal process • **Parent Process PID**: ID of the parent process • **Program Path of Parent Process**: program path of the parent process • **Behavior**: behavior of the abnormal process, for example, high CPU usage • **Number of Connections** • **CPU Usage Frequency** • **Status**: Event status. It can be **Handled** or **Unhandled**.	If abnormal process behaviors are detected, you are advised to check processes immediately. • If the processes are normal, ignore the event or whitelist the process. The processes will no longer trigger such events. • If the processes are unknown or malicious, you are advised to immediately kill them and isolate their source files. – You can isolate and kill detected or suspicious programs in one click. Alternatively, you can mark the event as **Handled**, immediately log in and stop the program, and scan the entire system for risks to prevent further damage. – HSS can isolate and kill malicious programs, including common ransomware, DDoS viruses, and Trojans. You are advised to enable this function to harden server security. For details, see **Isolating and Killing Malicious Programs**. • If the programs are harmless or mandatory for service operation, you can cancel isolation and restore the program source files.

Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Parameter	Suggestion
Critical file change	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Operation**: operation on a critical file • **File Path**: critical file path • **Move To**: path where the file is moved • **Directory**: whether the operation is performed on a directory. It can be **true** or **false**. • **Status**: Event status. It can be **Handled** or **Unhandled**.	If a key file change is detected, you are advised to check the change immediately. • If the change is valid, you can ignore the event. • If the change is invalid, critical files have been read, written, or deleted without authorization. You are advised to mark the event has **Handled** and immediately replace the file with the standard version of the OS. Log in to intruded accounts and change their passwords, and scan the entire system for risks to prevent further damage.
Web shell	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Trojan Path**: path of the Trojan file • **Discovered**: time when the Trojan file was discovered • **Status**: Event status. It can be **Handled** or **Unhandled**.	If a web shell is detected, you are advised to immediately check whether the file is valid. • If the file is valid, ignore the event or whitelist the file. The file will no longer trigger such events. • If the file is invalid, you are advised to mark the event as **Handled** and immediately isolate the file.
Reverse/ Abnormal shell	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **File Path**: shell file path • **Details** • **Status**: Event status. It can be **Handled** or **Unhandled**.	If a reverse or abnormal shell is detected, you are advised to check whether executed commands are valid. • If they are valid, you can ignore this event. • If they are invalid, mark the event as **Handled** and immediately log in to the system to block invalid connections or stop command execution, and scan the entire system for risks to prevent further damage.

 Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Parameter	Suggestion
High-risk command execution	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Hash**: hash value • **PID**: process ID • **Process Path** • **Process Command**: command that runs the process • **Parent Process PID**: ID of the parent process • **Parent Process Path** • **Parent Process Command**: command that runs the parent process • **Session Username**: name of the session user • **User**: responsible user • **Status**: Event status. It can be **Handled** or **Unhandled**.	If a high-risk command is detected, you are advised to immediately check whether the command is valid. • If it is valid, ignore the event or whitelist the command. The command will no longer trigger such events. • If it is invalid, mark the event as **Handled** and immediately log in to the system and check operations performed using the command, and scan the entire system for risks to prevent further damage.
Auto-startup check	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Service Name**: auto-started service name • **Path**: auto-started service path • **Type**: auto-started service type • **Event Type**: type of an event • **User**: responsible user • **File Hash**: hash value of a file • **Status**: Event status. It can be **Handled** or **Unhandled**.	If a new auto-started item is detected, you need to check whether the auto-startup item is valid. • If it is valid, ignore the event or whitelist the command. The command will no longer trigger such events. • If it is invalid, mark the event as **Handled** and immediately log in to the system to delete the item, and scan the entire system for risks to prevent further damage.

 Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Parameter	Suggestion
Unsafe account	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Account Name**: unsafe account name • **User Group**: user group of the unsafe account • **UID/SID** • **User Directory** • **Shell**: shell started by the user • **Status**: Event status. It can be **Handled** or **Unhandled**.	If an unsafe account is detected, you are advised to immediately check whether the account is valid. • If it is valid, you can ignore this event. • If it is invalid, mark the event as a **Handled** and perform the following operations: – Deleting suspicious accounts Delete unnecessary system login accounts, such as SSH accounts, from the servers. Delete unnecessary accounts used by the MySQL and FTP services from the servers. – Limiting account permissions Specify key configuration items to limit the file access and modification permissions of non-administrators, preventing unauthorized access and operations.
Privilege escalation	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Method**: privilege escalation method • **Affected File**: path of the file whose privileges are escalated • **Status**: Event status. It can be **Handled** or **Unhandled**.	If a privilege escalation operation is detected, you are advised to immediately check whether the operation is valid. • If it is valid, you can ignore this event. • If it is invalid, mark the event as **Handled** and immediately log in to the system to block invalid connections or stop command execution, and scan the entire system for risks to prevent further damage.

 Copyright © Huawei Technologies Co., Ltd.

Alarm Name	Parameter	Suggestion
Rootkit	• **Server Name**: affected server name • **IP Address**: IP address of the affected server • **Rootkit** • **Submodule** • **Description**: description on Rootkit features • **Status**: Event status. It can be **Handled** or **Unhandled**.	If Rootkit installation is detected, you are advised to immediately check whether the installation is valid. • If it is valid, you can ignore this event. • If it is invalid, mark the event as **Handled** and immediately log in to the system to stop Rootkit installation, and scan the entire system for risks to prevent further damage.

7.3 Managing Isolated Files

HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Events** page and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check them, and can recover isolated files anytime.

The following types of alarm events support online isolation and killing:

- Malicious program (cloud scan)
- Abnormal process behavior

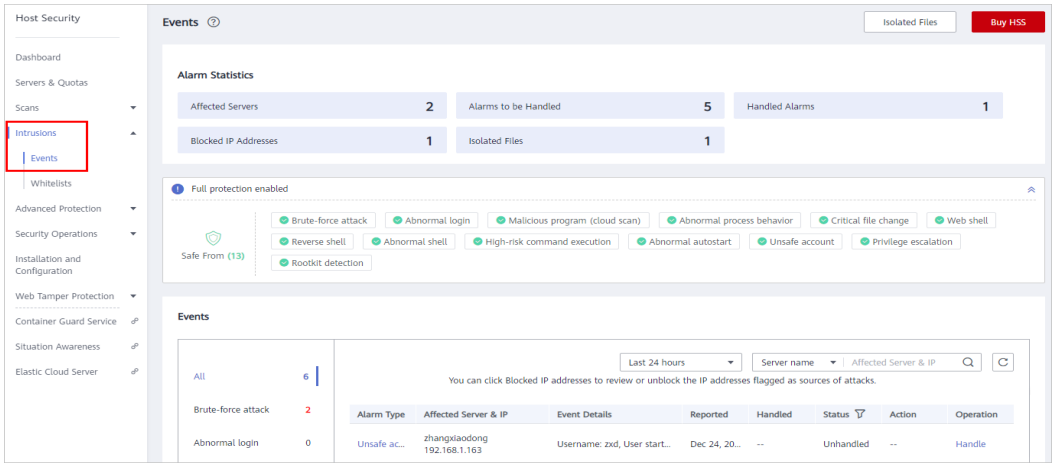
Isolating and Killing Files

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

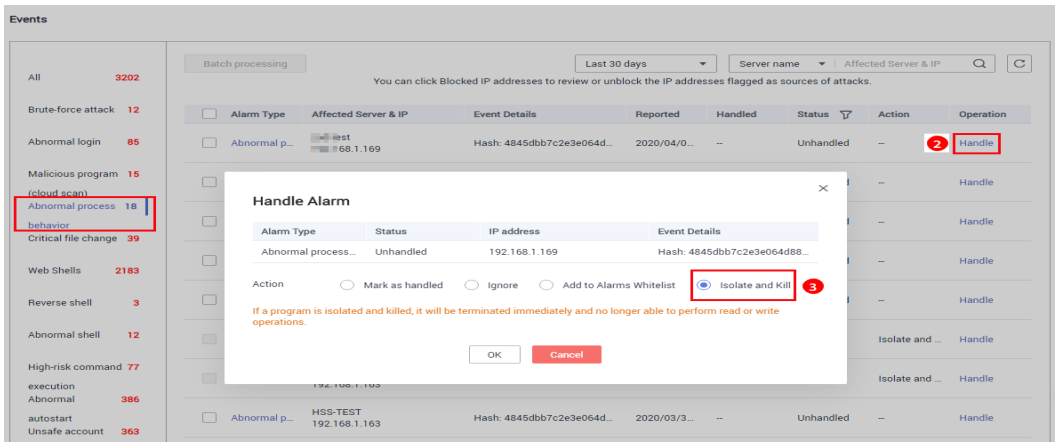
Step 3 In the navigation pane, choose **Intrusions** > **Events**.

Figure 7-6 Events page



Step 4 Select an event of the **Malicious program (cloud scan)** or **Abnormal process behavior** type, and click **Handle**. In the dialog box that is displayed, click **Isolate and Kill**.

Figure 7-7 Isolating and killing malicious programs



Step 5 Click **OK**. Files that have been isolated are displayed on a slide-out panel on the Events page and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check them.

----End

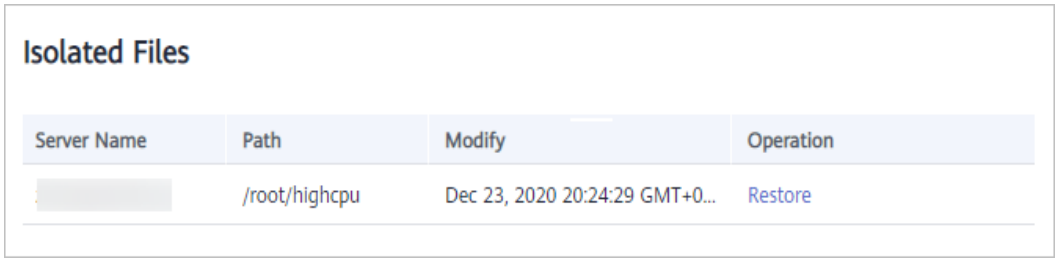
Checking Isolated Files

Step 1 On the **Events** page, click **Isolated Files** on the upper right corner.

Step 2 Check the servers, names, paths, and modification time of the isolated files, as shown in **Figure 7-8**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-8 Checking isolated files



----End

Recovering Isolated Files

Step 1 Click **Restore** in the **Operation** column of an isolated file.

Step 2 Click **OK**.

NOTE

Recovered files will no longer be isolated. Exercise caution when performing this operation.

----End

7.4 Configuring the Alarm Whitelist

You can configure the alarm whitelist to reduce false alarms. Events can be batch imported to and exported from the whitelist.

Whitelisted events will not trigger alarms.

On the **Events** page, you can add falsely reported alarms to the alarm whitelist. HSS will no longer generate alarms for it, and its statistics will not be displayed on the **Dashboard** page.

Only the enterprise and premium editions support whitelist management. The premium edition is provided for free if you have purchased the WTP edition.

Copyright © Huawei Technologies Co., Ltd.

Adding Events to the Alarm Whitelist

Table 7-3 Configuring the alarm whitelist

Method	Description
Add to alarm whitelist	Choose to add the alarm to the whitelist when handling it. For details, see **Checking and Handling Intrusion Events**. The following types of events can be added to the alarm whitelist: ● Reverse shell ● Web shell ● Abnormal process behavior ● Process privilege escalation ● File privilege escalation ● High-risk command ● Malicious program
Import the alarm whitelist	You can import whitelisted items on the **Alarm Whitelist** tab.

Checking the Alarm Whitelist

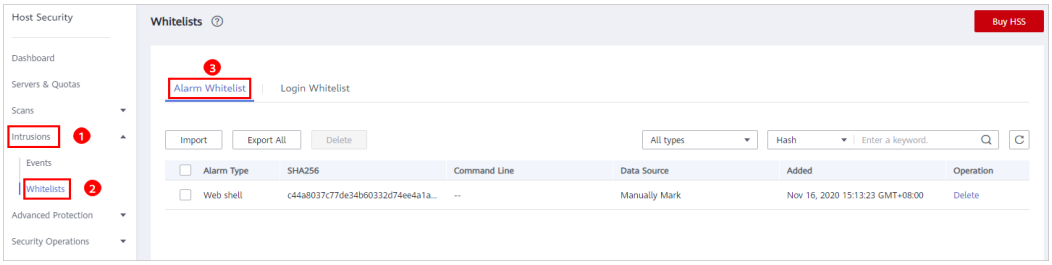
Perform the following steps to check the alarm whitelist:

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Whitelists** page, click **Alarm Whitelist**.

Figure 7-9 Alarm whitelist



----End

Importing and Exporting the Alarm Whitelist

You can import or export a whitelist for backup, restoration, or batch setting purposes.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

- The exported alarm whitelist is in .csv format.
- The settings will fail to be imported if you opened the .csv file in Excel or changed the content format.

  Format:

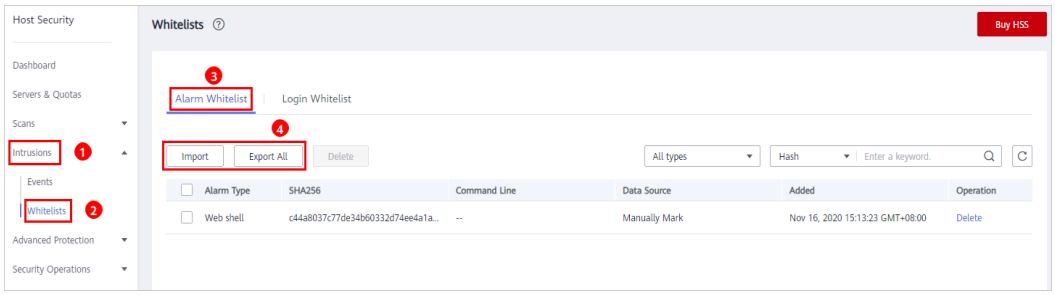
  "*Alarm_type*","*SHA256*","*Command_line*","*Data_source*","*Marking_time*"
  "webshell","66baecfe7208c00e139b898509626ee4d2ea81382ef15a4283b95d50f669b121","--","*File imported*","2020/02/28 07:32:44 GMT+08:00"
- The alarm whitelist supports incremental import. If the same record is imported again, only one entry will be displayed for it.

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Whitelists** page, click the **Alarm Whitelist** tab, as shown in **Figure 7-10**.

Figure 7-10 Clicking the Alarm Whitelist tab



- Click **Export All** to export the current alarm whitelist as a .csv file.
- Click **Import** and select the exported Excel file to import the alarm whitelist.

  In the displayed dialog box, click **Upload** and select a file. After the import is complete, you can check the imported alarms in the whitelist.

  NOTE

  - Only the files in CSV, TXT, or UTF-8 format can be imported and exported.
  - The file size cannot exceed 5 MB.
  - The file name can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

----End

Follow-Up Procedure

Removing alarms from the whitelist

To remove an alarm from the whitelist, select it and click **Delete**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Alarms removed from the whitelist will be triggered. Removals cannot be rolled back. Exercise caution when performing this operation.

7.5 Configuring the Login Whitelist

In the login whitelist, you can configure the IP addresses of destination servers, login IP addresses, and login usernames.

NOTE

- If the destination server IP address, login IP address, and username of a login are all whitelisted, this login will be allowed without checking.
- After an IP address is added to a whitelist by following the instructions in **Adding Login Information to the Login Whitelist**, the alarms (if any) that have been generated for the IP address will not be automatically cleared. Handle the alarms by referring to **Checking and Handling Intrusion Events**.

To add login information to the login whitelist, you can:

- Add false alarmed items of the **Brute-force attack** and **Abnormal login types** to the login whitelist when handling them. For details, see **Checking and Handling Intrusion Events**.
- Add it to the login whitelist on the **Login Whitelist** tab.

Only the enterprise and premium editions support whitelist management. The premium edition is provided for free if you have purchased the WTP edition.

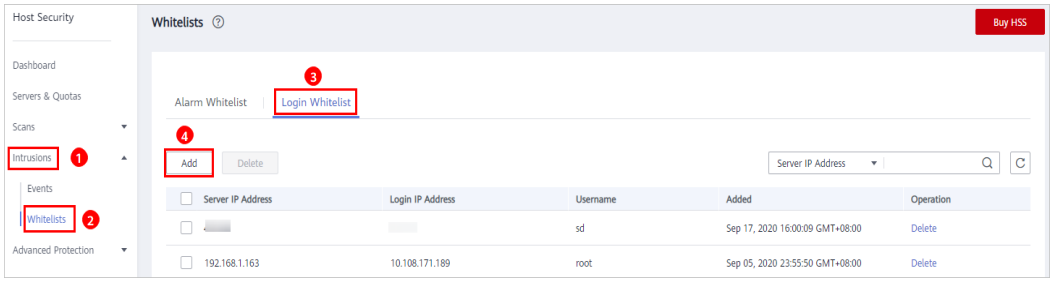
Adding Login Information to the Login Whitelist

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Whitelists** page, click the **Login Whitelist** tab and click **Add**, as shown in **Figure 7-11**.

Figure 7-11 Login whitelist



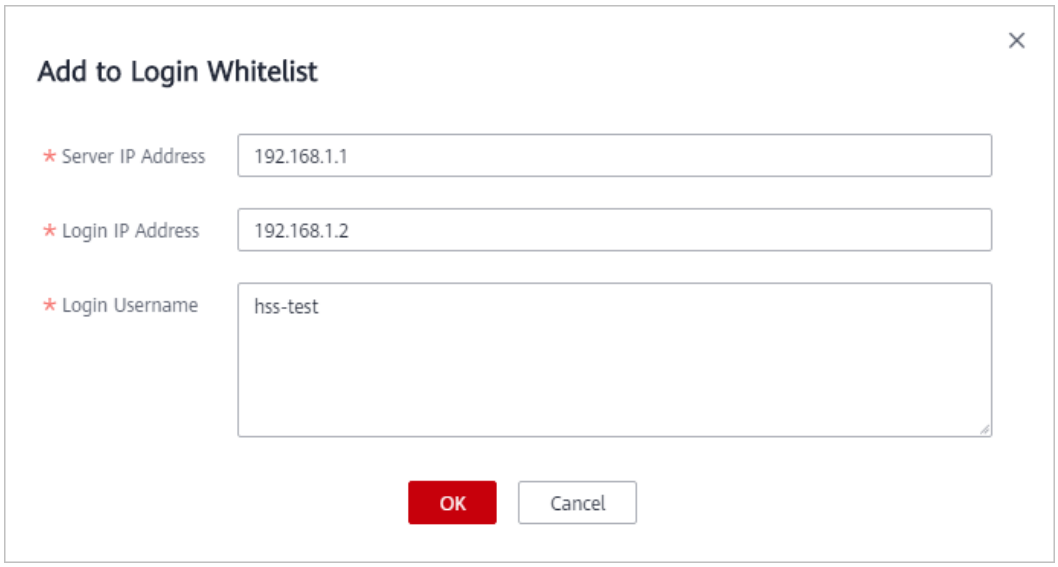
Step 4 In the **Add to Login Whitelist** dialog box, enter the server IP address, login IP address, and login username, as shown in **Figure 7-12**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The IP addresses can be IPv4 or IPv6 addresses.
- You can enter one or more values in each IP address text box. IP addresses, ranges, and masks are supported, and should be separated by commas (,). Example: **192.168.1.1, 192.168.2.1-192.168.6.1, 192.168.7.0/24**.
- The allowed maximum length of server IP addresses or login IP addresses is 128 bytes.

Figure 7-12 Adding login information to the login whitelist



Step 5 Click **OK**.

----End

Other Operations

Removing login information from login whitelist

To delete a piece of login information from the whitelist, select it and click **Delete**, or click **Delete** in the row it resides.

NOTE

Exercise caution when performing the deletion operation because it cannot be rolled back.

 Copyright © Huawei Technologies Co., Ltd.

8 Advanced Protection

8.1 Application Recognition Service

8.1.1 Checking the Whitelist Policy List

Application Recognition Service (ARS) scans all the applications running on your servers for uncertified or unauthorized applications, helping you maintain a secure runtime.

Scenario

Set whitelist policies, and determine whether applications are **Trusted**, **Untrusted**, or **Unknown**. The applications that are not whitelisted are not allowed to run. This function protects your servers from untrusted or malicious applications, reducing unnecessary resource usage.

You can create a whitelist policy and apply it to your servers. HSS will check whether suspicious or malicious processes exist on the servers, and generate alarms or isolate the processes that are not in the whitelist.

NOTE

- An alarm is generated when an application not in the whitelist is started.
- An application not in the whitelist is probably a new normal application, or a malicious program implanted through intrusion.
  - If the alarmed application is normal, frequently used, or a third-party application you installed, you are advised to add it to the whitelist. HSS will no longer report alarms when the application starts.
  - If the application is malicious, you are advised to delete it in a timely manner and check whether your configuration files, such as scheduled task files, have been tampered with.

Checking the Whitelist Policy List

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

 Copyright © Huawei Technologies Co., Ltd.

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Programs** page, click the **Whitelist Policies** tab, as shown in **Figure 8-1**.

Figure 8-1 Checking the whitelist policy list

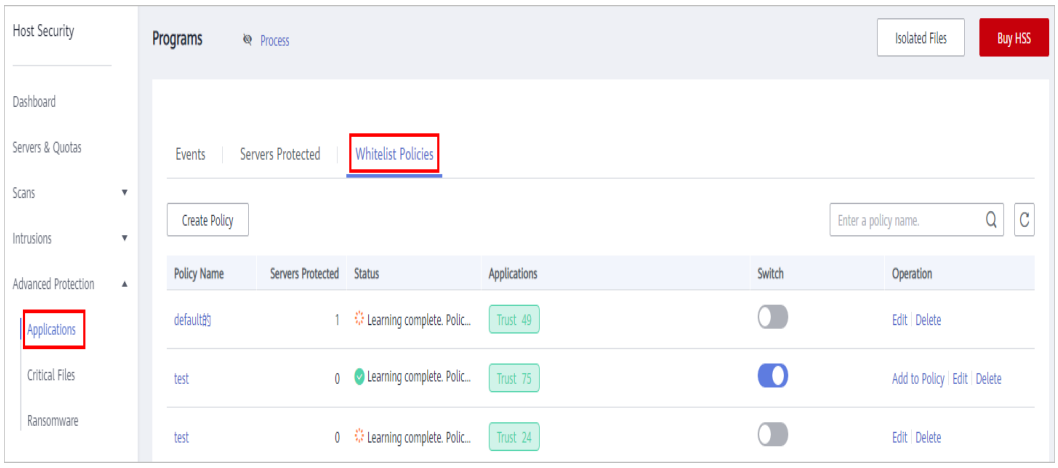


Table 8-1 Policy list parameters

Parameter	Description
Policy Name	Whitelist policy name
Servers Protected	Number of servers where the whitelist policy takes effect
Status	Policy status. Its value can be: • Learning Intelligent learning is in progress. After a policy is created, the intelligent learning function automatically analyzes operations on the servers you selected. The status of a new policy is **Learning**. • Learning complete. Policy not in effect Intelligent learning is complete. You need to manually enable the policy for it to take effect. To enable the policy, click in the row where it locates. HSS will automatically check whether the application running on your servers are trustworthy, and mark them as trusted, untrusted, or unknown. • Learning complete. Policy in effect Intelligent learning is complete. The policy has taken effect on associated servers.
Applications	Number of trusted, untrusted, and unknown applications identified by HSS

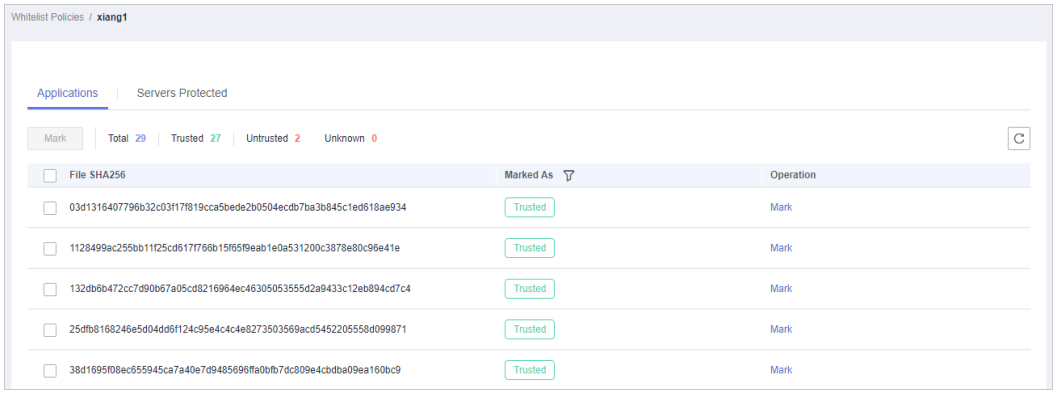
 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Switch	Enables or disables a policy. If the policy is in the **Learning complete. Policy not in effect** state, you can click to enable it. The whitelist policy takes effect only after it is enabled.
Operation	Operations that can be performed on the policy, including: • **Applications**. You can click this button to select servers that a policy applies to. • **Edit**. You can click this button to modify the period and servers for intelligent learning. • **Delete**: You can click this button to delete a whitelist policy. After a whitelist policy is deleted, the applications on the servers associated to it will no longer be protected.

Step 4 Click the name of a whitelist policy to view the applications on associated servers, as shown in **Figure 8-2**.

The total number of applications, number of trusted applications, number of untrusted applications, and number of unknown applications are displayed. You can mark an application as trusted, untrusted, or unknown, and create an application whitelist for the application.

Figure 8-2 Application list



Step 5 Click the **Servers Protected** tab to view the servers that the whitelist policy applies to, as shown in **Figure 8-3**.

The server names and IP addresses, whitelist policy, number of suspicious operations, and the way to handle the operations are displayed.

- **Suspicious Operations** include startup of processes that are not in the whitelist policy or marked as **Untrusted** or **Unknown**.
- **Action** in the following figure indicates that HSS will report an alarm when detecting suspicious operations.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-3 Checking protected servers

NOTE

You can remove servers as required. Servers removed will no longer be protected by the whitelist policy.

----End

8.1.2 Applying a Whitelist Policy

You can apply whitelist policies to your servers. A machine learning engine will automatically analyze operations performed on the servers. In this way, HSS will check whether suspicious or malicious processes exist on your servers, and report alarms on or isolate the processes that are not in the whitelist.

Prerequisites

- The premium edition has been enabled.
- The server you want to apply the policy to is in the **Running** state, its agent is in the **Online** state, and the premium edition has been enabled for the server.
- Only one whitelist policy can be applied to a server.

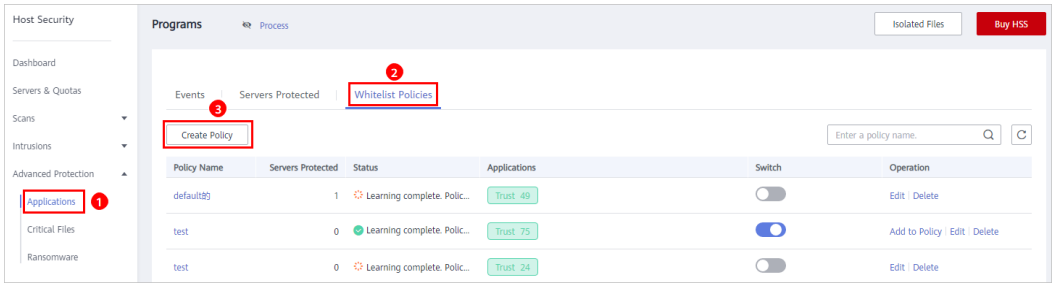
Creating a Whitelist Policy

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Programs** page, click the **Whitelist Policies** tab, and click **Create Policy**, as shown in **Figure 8-4**.

Figure 8-4 Creating a whitelist policy



Step 4 Set policy details, as shown in **Figure 8-5**.

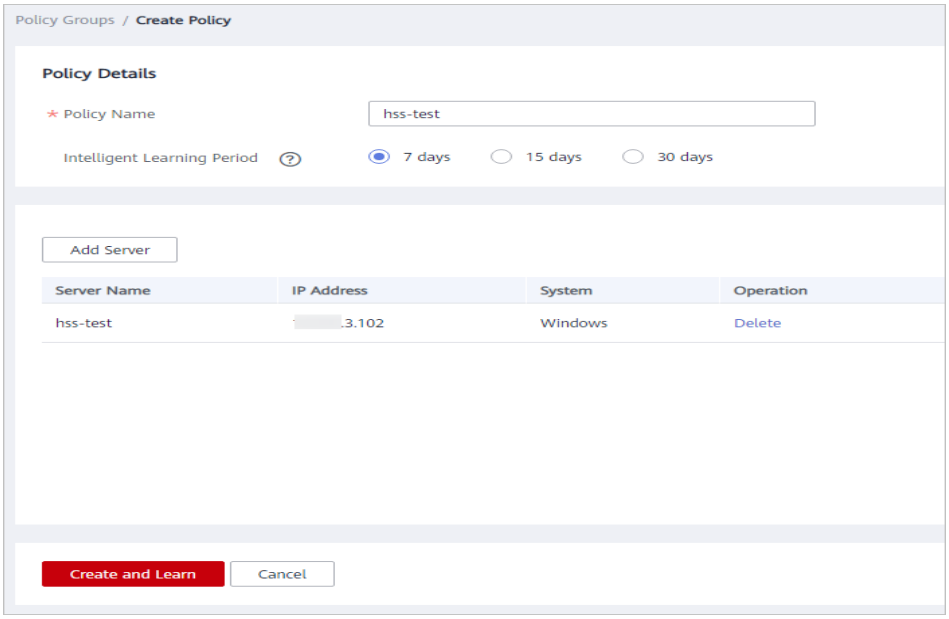
- **Policy Name**: Set a policy name.

Copyright © Huawei Technologies Co., Ltd.

- **Intelligent Learning Period**: Select **7 days**, **15 days**, or **30 days**.

  The period you select must be long enough for the policy to learn about all the common operations performed on your servers. Otherwise, intelligent learning results will be inaccurate.

Figure 8-5 Configuring a policy



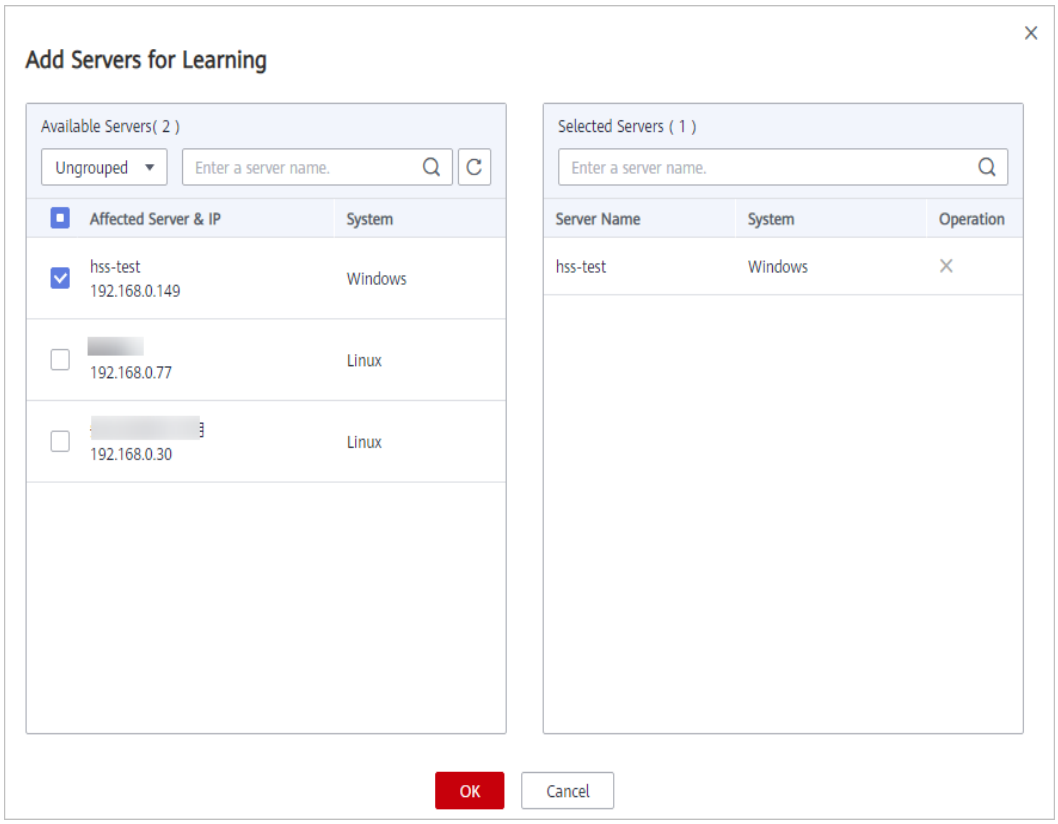
Step 5 Click **Add Server** to add an intelligent learning server, as shown in **Figure 8-6**.

NOTICE

- The server you want to apply the policy to must be in the **Running** state, its agent must be in the **Online** state, and the premium edition must be enabled for the server.
- You can add one or more servers. HSS will learn operations performed on them and identify trusted, untrusted, and unknown applications.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-6 Adding servers for policy learning



Step 6 Click **OK**.

- In the server list, you can view the service name, IP address, and system of each server.
- You can add or remove learning servers as required.

Step 7 Click **Create and Learn**.

In the whitelist policy list, you can view the policy name, protected servers, policy status, applications, and whether a policy is enabled.

Step 8 Wait until the whitelist policy learning is complete and the policy status becomes **Learning complete. Policy not in effect**, and click to enable the whitelist policy.

After the whitelist policy is enabled, if its status becomes **Learning complete. Policy in effect**, the whitelist policy is successfully created.

----End

Associating Servers

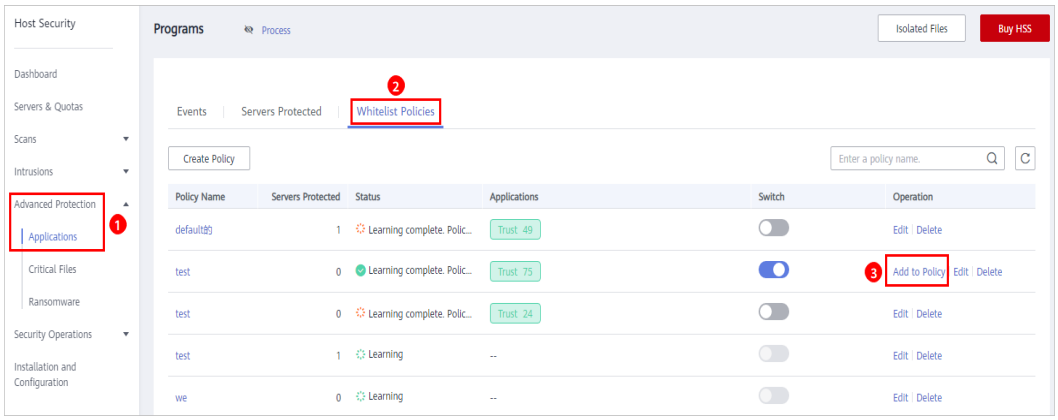
After a whitelist policy is created, you can associate servers with it. HSS will check for suspicious or malicious processes on the associated servers.

You can only associate servers with a whitelist policy whose status is **Learning complete. Policy in effect**.

 Copyright © Huawei Technologies Co., Ltd.

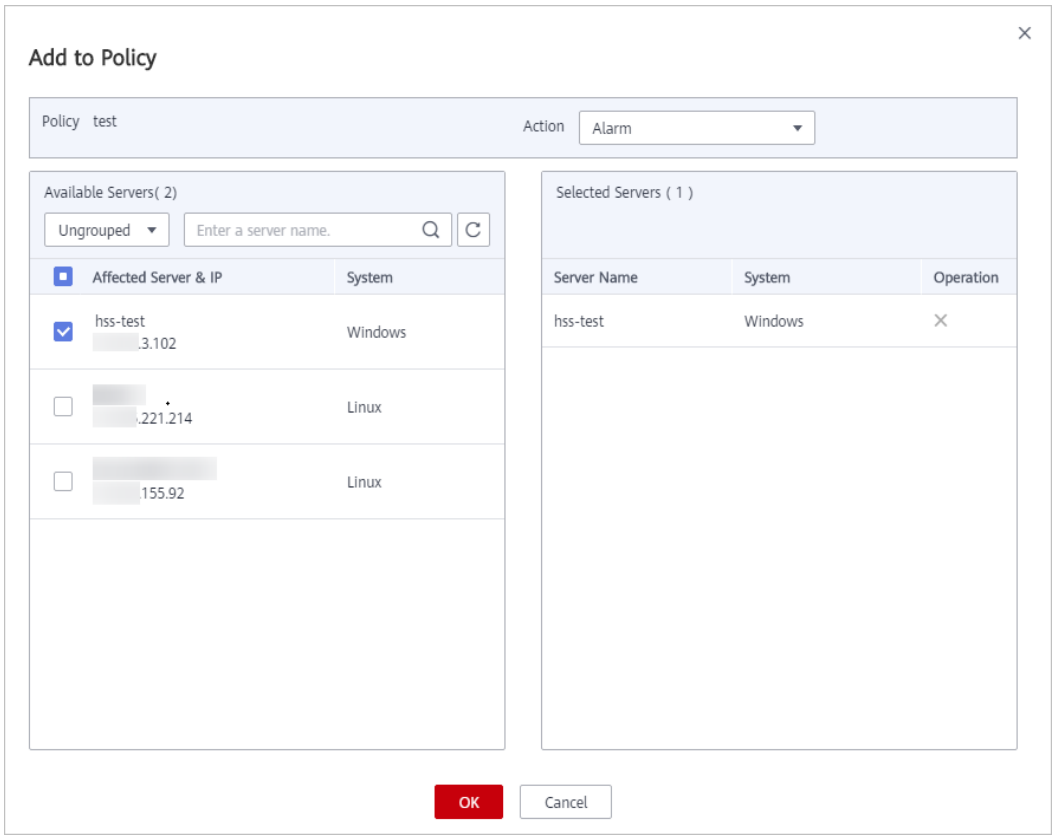
Step 1 Click **Applications**, as shown in **Figure 8-7**.

Figure 8-7 Associating servers



Step 2 In the displayed dialog box, select **Alarm** for **Action** and select servers, as shown in **Figure 8-8**.

Figure 8-8 Selecting servers



Step 3 Click **OK**.

The number of servers associated with the whitelist policy will be displayed in the whitelist policy list.

----End

 Copyright © Huawei Technologies Co., Ltd.

Follow-Up Procedure

Managing protected servers

- To add servers, click the **Servers Protected** tab and click **Add to Policy**.

  You can check the server names and IP addresses, whitelist policy, number of suspicious operations, and the way to handle the operations.
- To remove a protected server, click **Delete** in the **Operation** column. After a whitelist policy is deleted, the applications on the servers associated to it will no longer be protected.

Editing a whitelist policy

You can click **Edit** to modify the period and servers for intelligent learning.

Exercise caution when modifying the intelligent learning period of a policy. Before the learning completes, servers associated to the policy are not protected.

Deleting a whitelist policy

You can click the **Delete** button to delete a whitelist policy.

8.1.3 Checking and Handling Application Events

If a whitelist policy takes effect on your servers, HSS will check and mark applications as trusted, untrusted, or unknown, and report alarms on or isolate the applications that are not in the whitelist.

You can manually mark alarmed applications as trusted, untrusted, or unknown.

If you determine that a program is a malicious, you can manually isolate and kill it. When an application is isolated and killed, it is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious applications (if any).

The event management list displays untrusted and unknown applications, and the applications that are not in the whitelist policy.

NOTE

You are advised to check and handle the alarmed applications in a timely manner.

ARS is a trial function in the current version. To use stronger functions, purchase HSS (New).

Checking Application Events

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Programs** page, click the **Events** tab, as shown in **Figure 8-9**.

Figure 8-9 Application event management page

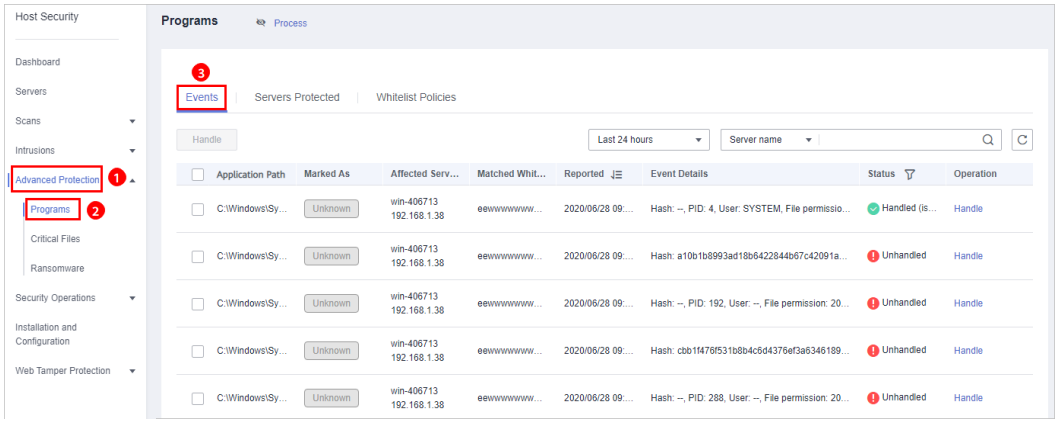


Table 8-2 Application event parameters

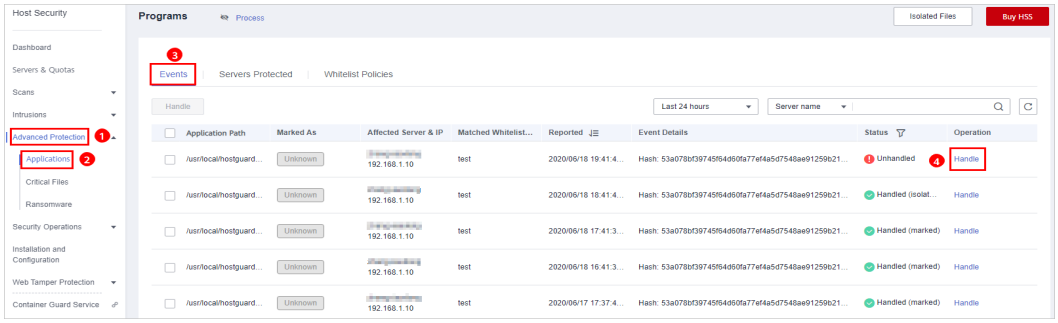
Parameter	Description
Program Path	Path of an application
Marked As	Application status. It can be **Trusted**, **Untrusted**, or **Unknown**.
Affected Server & IP	Name and IP address of an affected server
Matched Whitelist Policy	Whitelist policy that matches an alarm
Reported	Time when an alarm is reported
Event Details	Brief description of an alarm event
Status	Application event status. Its value can be **Handled** or **Unhandled**.

----End

Handling Application Events

Step 1 In the **Operation** column of an event, click **Handle**, as shown in **Figure 8-10**.

Figure 8-10 Handling an application event



Copyright © Huawei Technologies Co., Ltd.

Step 2 In the displayed **Handle Event** dialog box, select an action, as shown in **Figure 8-11**.

Figure 8-11 Handling an application event

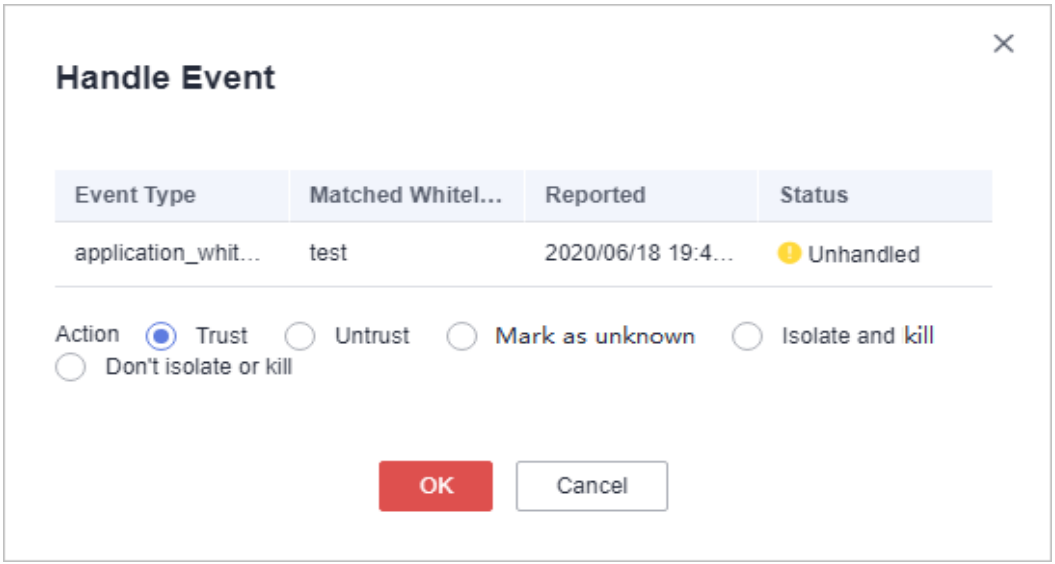


Table 8-3 Event handling actions

Action	Description
Trust	Marks an application as trusted. The application startup will no longer trigger alarms.
Untrust	Marks an application as untrusted. The application startup will trigger alarms.
Mark as unknown	Marks an application as unknown. The application startup will trigger alarms.
Isolate and kill	If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check the files. For details, see **Managing Isolated Files**. **NOTE** When an application is isolated and killed, it is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious files (if any).
Don't isolate or kill	Cancels the isolation and killing of an application. **NOTE** Exercise caution when performing this operation. If you restore a malicious application, it will harm your servers.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Click **OK**.

----End

8.2 File Integrity Monitoring

8.2.1 Adding a Monitored File

File integrity monitoring (FIM) checks the files in your OSs, applications, and other components for tampering, helping you meet PCI-DSS requirements.

FIM compares files with their versions in the previous scan to check whether files have been modified, and whether the modifications are suspicious.

FIM checks the integrity of Linux files and manages operations on them, including:

- Create and delete files
- Modify files (changes in file size, ACLs, and content hashes)

The registry monitoring function will be available soon.

NOTICE

You are advised to monitor only the files that are important for systems and applications, and are rarely modified.

If you monitor files that are frequently modified, by applications or OSs, such as log files and text files, a lot of false alarms will be generated.

Enabling FIM

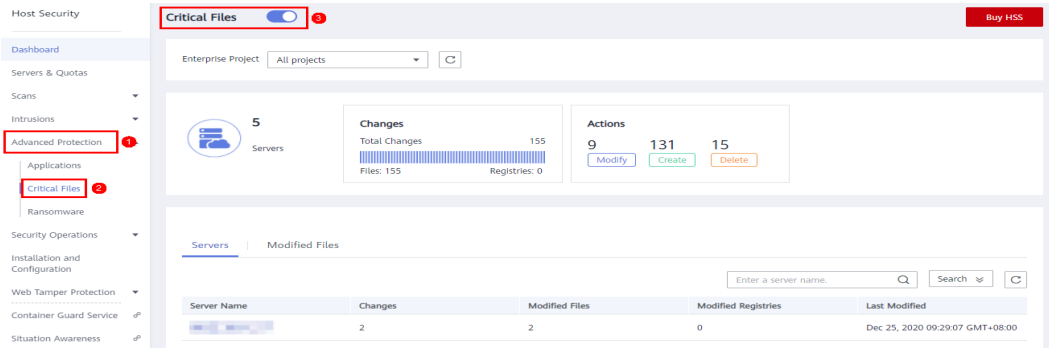
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Critical Files** page, click to enable FIM, as shown in **Figure 8-12**.

The default setting is .

Figure 8-12 Enabling FIM



 Copyright © Huawei Technologies Co., Ltd.

Step 4 Check the total number of servers, number of modified files, types of modifications, risks, affected servers, and modified files.

----End

Adding a Monitored File

To add a management file, ensure that:

- You have deployed the **File Integrity Monitoring** policy on servers.
- The **File Integrity Monitoring** policy has been enabled.

Perform the following steps to add a monitored file:

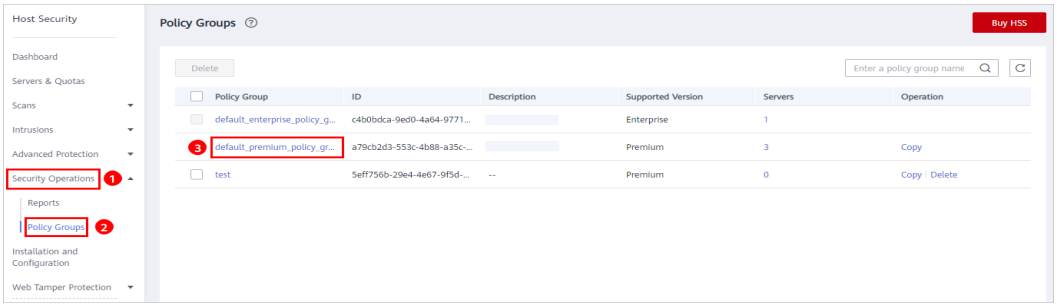
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Security Operations** > **Policy Groups**.

Step 4 On the **Policy Groups** page, click the policy group deployed on your servers. Take the default policy group of the premium edition as an example, as shown in **Figure 8-13**.

Figure 8-13 Default policy group

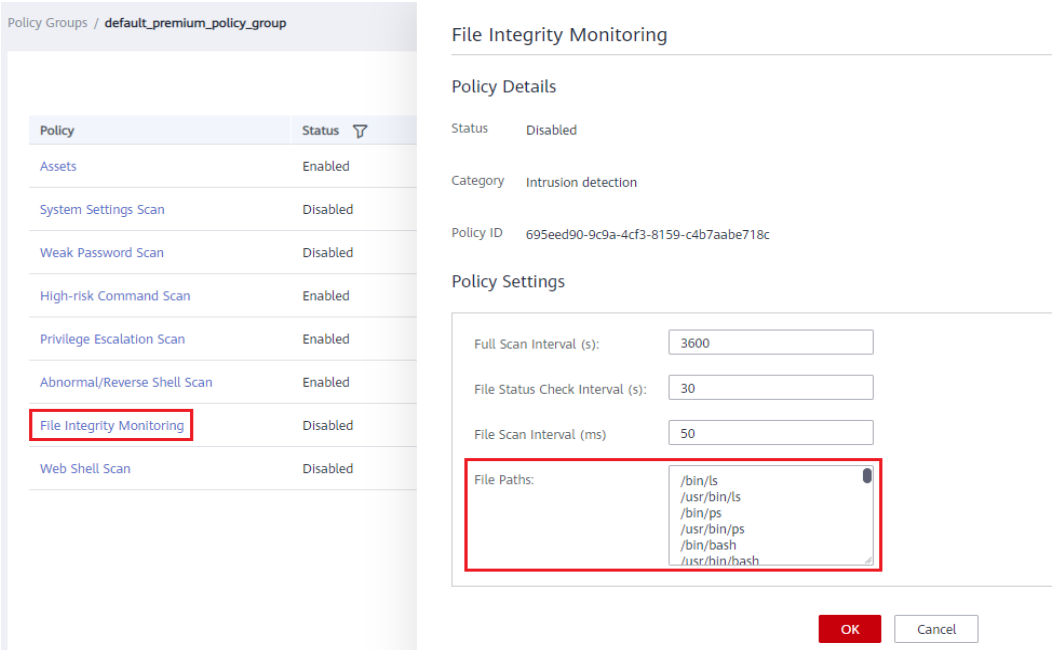


Step 5 Click **File Integrity Monitoring** and set monitored files, as shown in **Figure 8-14**.

For details about how to configure the **File Integrity Monitoring** policy, see **File Integrity Monitoring**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-14 File Integrity Monitoring policy



Step 6 Click **OK**.

----End

Follow-Up Procedure

Disabling FIM

To disable FIM, click  . If the function is disabled, HSS no longer monitors your files or displays FIM statistics.

8.2.2 Checking Change Statistics

You can check the number and types of changes, the number of modified files and registries on a server, and change details to find malicious changes in a timely manner.

Checking Change Statistics

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Go to the **Critical Files** page to check change statistics, as shown in **Figure 8-15**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-15 Checking change statistics

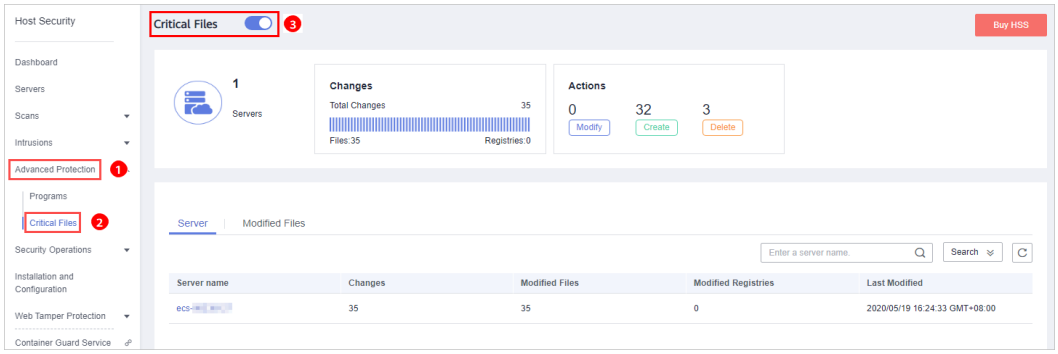


Table 8-4 Change statistics

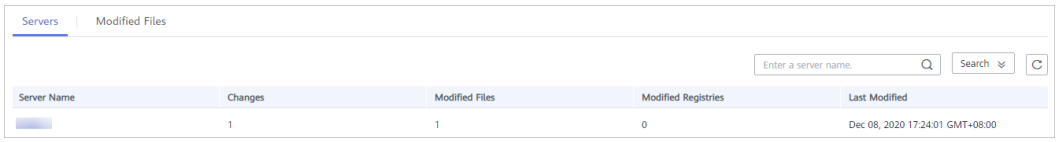
Item	Description
Servers	Total number of managed servers
Changes	• **Changes**: total number of modifications in monitored files • **Files**: total number of files • **Registries**: total number of registries
Actions	• **Modify**: total number of changes in monitored files • **Create**: total number of created files • **Delete**: total number of deleted files

----End

Checking Modified Files on a Single Server

Step 1 In the server list, check modified files and registries on a server, and the time when they were modified.

Figure 8-16 Server list



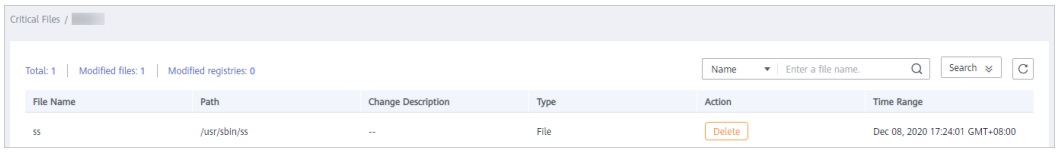
Step 2 Click a server name and check its change statistics above the displayed list, including the total number of changes, number of modified files, and number of modified registries, as shown in **Figure 8-17**.

NOTE

You can click **Search** to expand the advanced search area. Here you can search for a server by its name and the time when changes were made.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-17 Server change details



Step 3 Check the change details of the files and registries in the file list of the server.

The details include including the file and registry names and types, paths, changed content, actions, and time when changes were made.

NOTE

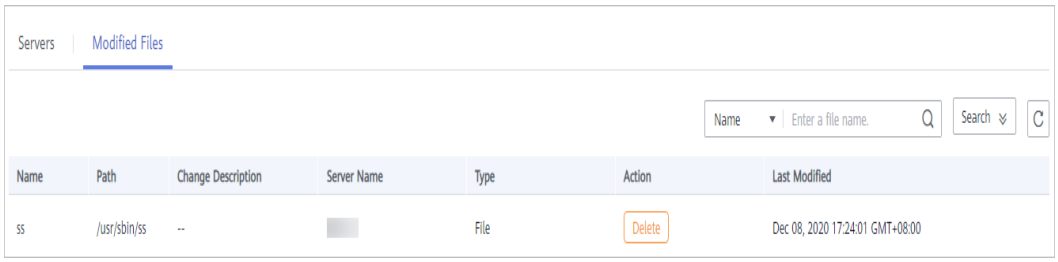
- You can enter a name or path to search for a file or registry.
- You can click **Search** to expand the advanced search area. Here you can search for a server by **Name**, **Path**, **Type**, **Action**, and **Time Range**.

----End

Checking All the Modified Files

You can check all the change files and registries on your servers, including their names, paths, description, server names, actions, and the time when they were changed, as shown in **Figure 8-18**.

Figure 8-18 Modified files



NOTE

- You can enter a name or path to search for a file or registry.
- You can click **Search** to expand the advanced search area. Here you can search for a server by **Name**, **Path**, **Type**, **Action**, and **Time Range**.

8.3 Ransomware Prevention

8.3.1 Ransomware Prevention

Ransomware is malicious software that infects your servers, encrypts your files, and demands a ransom in order for your files to be decrypted. You can use HSS to defend against ransomware before, during, and after server intrusion and protect your business.

 Copyright © Huawei Technologies Co., Ltd.

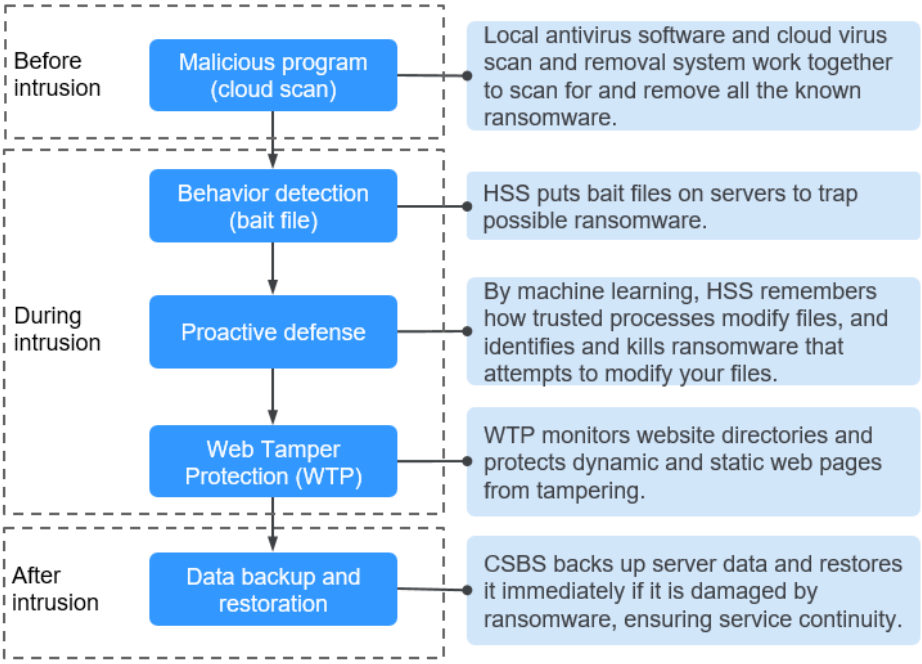
NOTE

Ransomware prevention is a trial function in the current version. To use stronger functions, purchase HSS (New).

How HSS Prevents Ransomware

HSS monitors critical files stored on your servers and prevents unauthorized applications from encrypting or modifying the files, protecting your servers from ransomware. HSS can also put bait files on your servers to trap and kill ransomware. To better protect your services, you can use Cloud Server Backup Service (CSBS) to back up your server data, and recover the data to avoid service interruption in the case of an intrusion.

Figure 8-19 How HSS prevents ransomware



Functions

You can create a ransomware protection policy. The policy will learn and analyze operations on servers, identify trusted applications, and remember how trusted processes modify your files. After the learning completes, HSS automatically applies the policy to the servers you specified, and reports alarms on untrusted applications.

- Linux ransomware prevention
  - If you enable bait protection in a Linux protection policy, HSS will put a bait file on each protected server. Ransomware attempting to encrypt bait files will trigger alarms immediately.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Bait files are marked by HSS. While you handle suspicious files, be careful not to delete the bait files by mistake.
- Bait files will neither affect your services nor trigger malicious behaviors. If the bait files are deleted, HSS will be unable to trap and kill ransomware.

– If you create a Linux protection policy, HSS will learn how trusted processes modify files on protected servers, and report alarms on the ransomware not trapped by bait files.

- Windows ransomware prevention

  If you create a Windows protection policy, HSS will learn how trusted processes modify files on protected servers, and report alarms on modifications made by untrusted processes.

8.3.2 Creating a Protection Policy

To protect your servers from ransomware, you can create a policy, set critical file paths in the policy, and enable machine learning.

Machine learning automatically collects and aggregates normal application behavior on the servers associated with the policy. Operations on files performed by untrusted applications or applications that are not specified in the policy will trigger alarms.

NOTE

Ransomware prevention is a trial function in the current version. To use stronger functions, purchase HSS (New).

Prerequisites

- The enterprise or WTP edition HSS has been enabled.
- The **Agent Status** of the Linux server is **Online**.

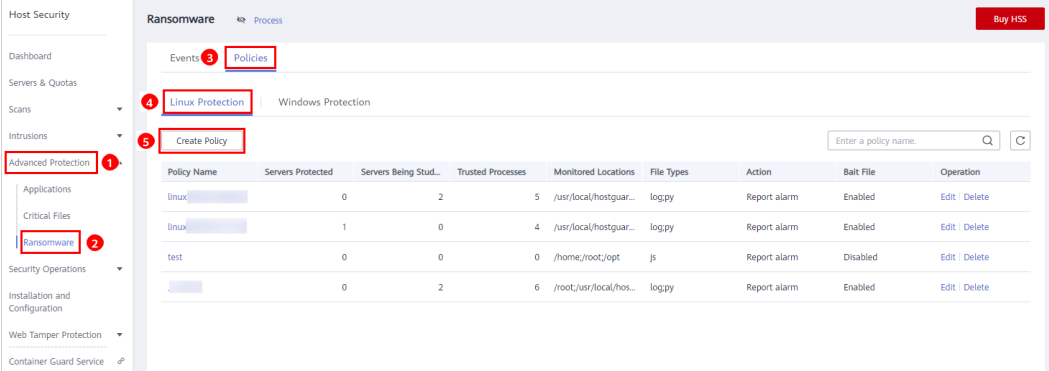
Creating a Linux Protection Policy

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Ransomware** page, click the **Policies** tab, and click **Create Policy**, as shown in **Figure 8-20**.

Figure 8-20 Linux protection policy page



Step 4 Set policy details, as shown in **Figure 8-21**.

Figure 8-21 Configuring the Linux protection policy

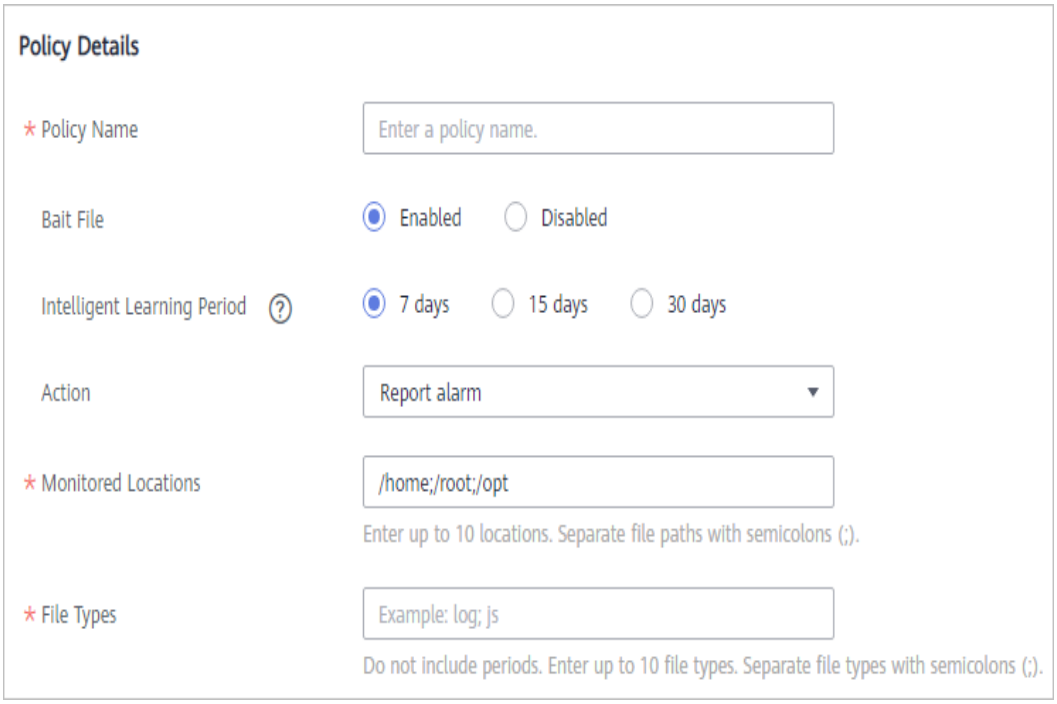


Table 8-5 Policy parameters

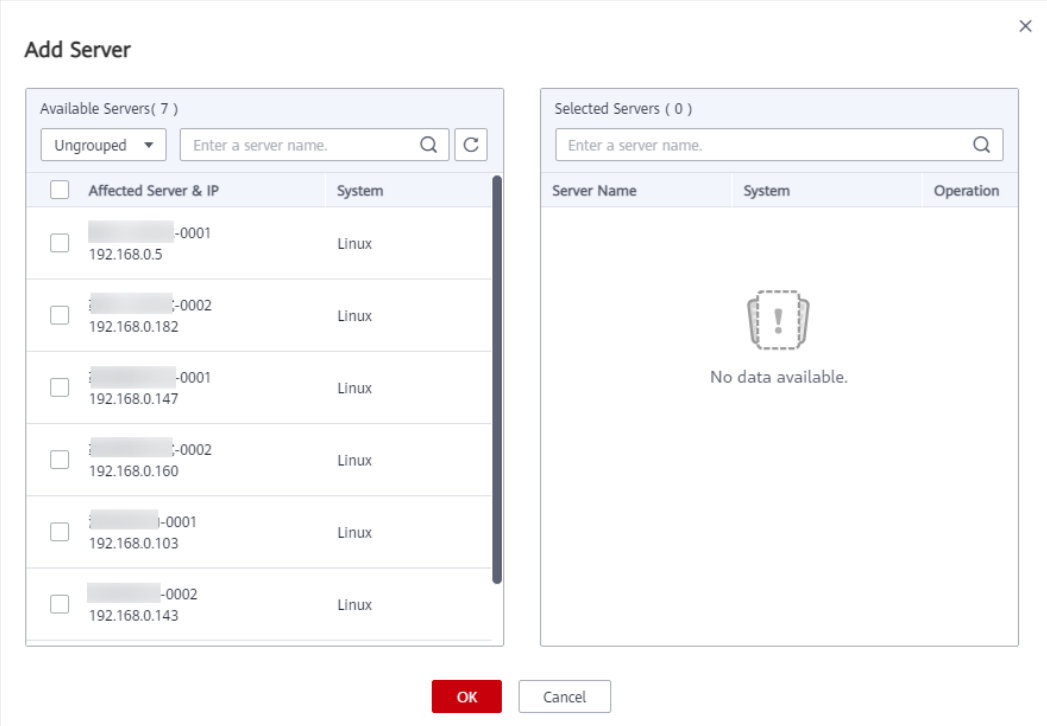
Parameter	Description
Policy Name	Ransomware prevention policy name
Bait File	If you enable the bait file function, HSS will put a bait file on each protected server to trap and kill ransomware.
Intelligent Learning Period	Select **7 days**, **15 days**, or **30 days**. HSS uses a machine learning engine to identify if an application has possibly tampered with any of the files on your servers.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Action	Action taken when suspicious operations on monitored files are detected. For example, report alarms.
Monitored Locations	Path of monitored files. Multiple paths are separated by semicolons (;). Operations on the files in these paths are monitored. Example: **/opt;/opt/sap** **NOTE** You are advised to configure this parameter to specific file paths. To protect all paths, set this parameter to **--**.
File Types	Extension of monitored files. Multiple paths are separated by semicolons (;). Example: **sql;txt;sh**

Step 5 Click **Add Server**. In the displayed **Add Server** dialog box, select associated servers, as shown in **Figure 8-22**.

Figure 8-22 Associating Linux servers



Step 6 Click **OK**.

NOTE

- You can check the name, IP address, and system of the associated server.
- To remove an associated server, click **Delete** in the **Operation** column.

Step 7 Click **Create and Learn**.

Created policies will be displayed in the policy list, as shown in **Figure 8-23**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-23 Linux protection policy list

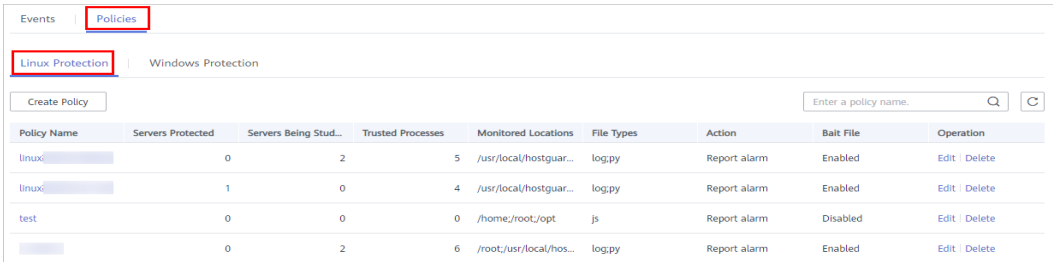


Table 8-6 Policy list parameters

Parameter	Description
Policy Name	Intelligent learning policy name
Servers Protected	Number of servers protected by the policy
Servers Being Studied	Number of servers where the learning is performed
Trusted Processes	Number of trusted processes. After the intelligent learning policy takes effect, HSS automatically identifies and counts trusted processes on your server.
Monitored Locations	Locations of monitored files
File Types	Extensions of monitored files
Action	Action taken when suspicious operations on monitored files are detected. Example: **Report alarm**
Bait File	• **Enabled**: The bait file function is enabled. HSS puts a bait file on each protected server. Ransomware attempting to encrypt bait files will trigger alarms immediately. • **Disabled**: The bait file function is disabled.

----End

Creating a Windows Protection Policy

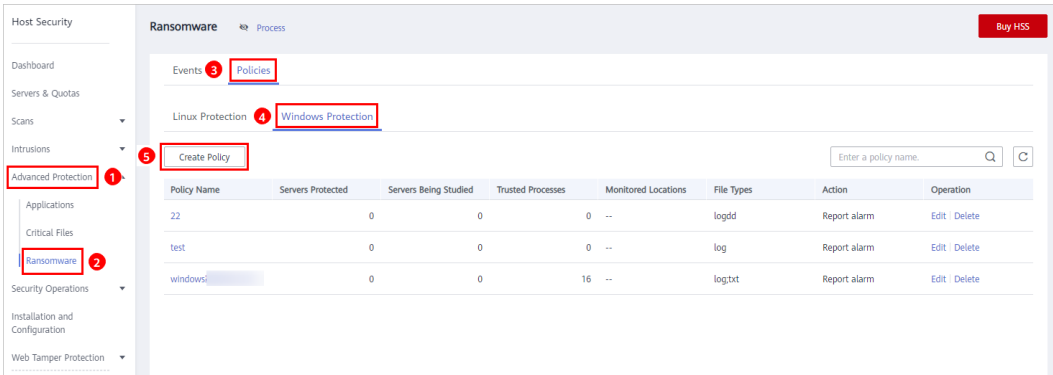
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Ransomware** page, click the **Policies** tab, and click **Create Policy**, as shown in **Figure 8-24**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-24 Windows protection policy list



Step 4 Set policy details, as shown in **Figure 8-25**.

Figure 8-25 Configuring the Windows protection policy

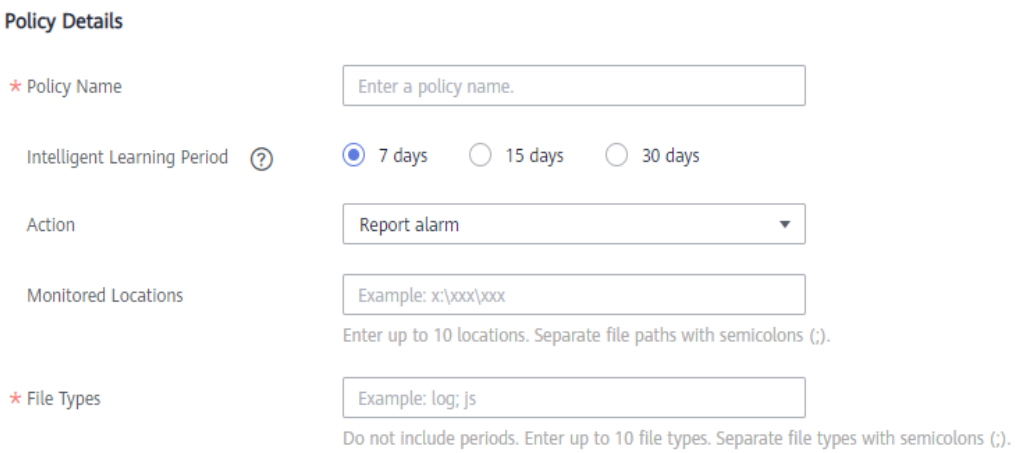


Table 8-7 Basic information parameters

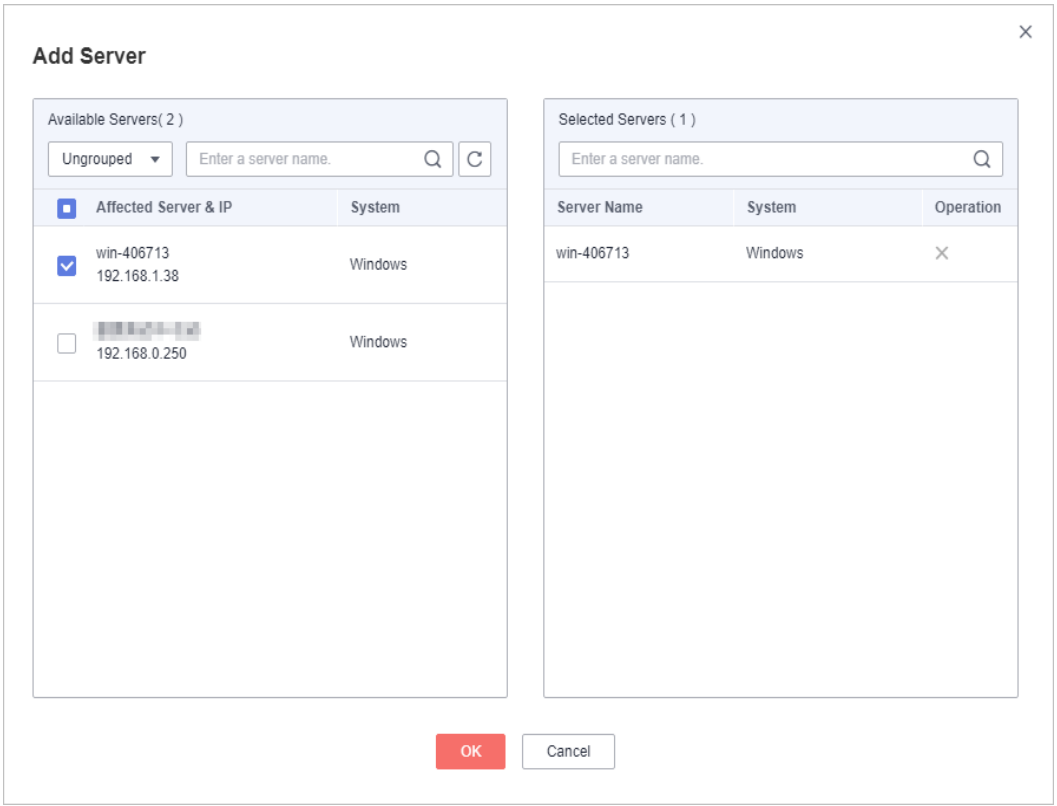
Parameter	Description
Policy Name	Ransomware prevention policy name
Intelligent Learning Period	Select **7 days**, **15 days**, or **30 days**. HSS uses a machine learning engine to identify if an application has possibly tampered with any of the files on your servers.
Action	Action taken when suspicious operations on monitored files are detected. For example, report alarms.
Monitored Locations	Path of monitored files. Multiple paths are separated by semicolons (;). Operations on the files in these paths are monitored. If no paths are specified, all the files on the servers associated to the policy are monitored.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
File Types	Extension of monitored files. Multiple paths are separated by semicolons (;).

Step 5 Click **Add Server**. In the displayed **Add Server** dialog box, select associated servers, as shown in **Figure 8-26**.

Figure 8-26 Associating Windows servers



Step 6 Click **OK**.

NOTE

- You can check the name, IP address, and system of the associated server.
- To remove an associated server, click **Delete** in the **Operation** column.

Step 7 Click **Create and Learn**.

Created policies will be displayed in the policy list, as shown in **Figure 8-27**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-27 Windows protection policy list

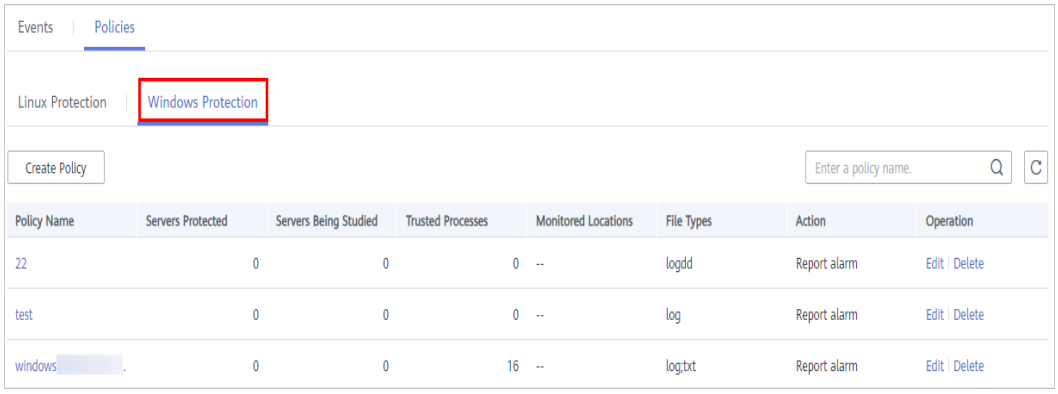


Table 8-8 Policy list parameters

Parameter	Description
Policy Name	Intelligent learning policy name
Servers Protected	Number of servers protected by the policy
Servers Being Studied	Number of servers where the learning is performed
Trusted Processes	Number of trusted processes. After the intelligent learning policy takes effect, HSS automatically identifies and counts trusted processes on your server.
Monitored Locations	Path of monitored files. Multiple paths are separated by semicolons (;). Operations on the files in these paths are monitored. If no paths are specified (**--** is displayed), all the files on the servers associated to the policy are monitored.
File Types	Extension of monitored files. Multiple paths are separated by semicolons (;).
Action	Action taken when suspicious operations on monitored files are detected. For example, report alarms.

----End

8.3.3 Managing Protection Policies

A machine learning engine identifies whether an application has possibly tampered with any of the files on your servers based on the policies you enabled. After the learning completes, the policy automatically takes effect on associated servers.

 Copyright © Huawei Technologies Co., Ltd.

You can modify the basic information or associated servers of a policy in the policy list.

NOTE

Ransomware prevention is a trial function in the current version. To use stronger functions, purchase HSS (New).

Prerequisites

The server is in the **Running** state, and its agent is in the **Online** state.

Checking Protection Policies

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Ransomware** page, click the **Policies** tab. The ransomware prevention policy list is displayed, as shown in **Figure 8-28**.

Figure 8-28 Policy list

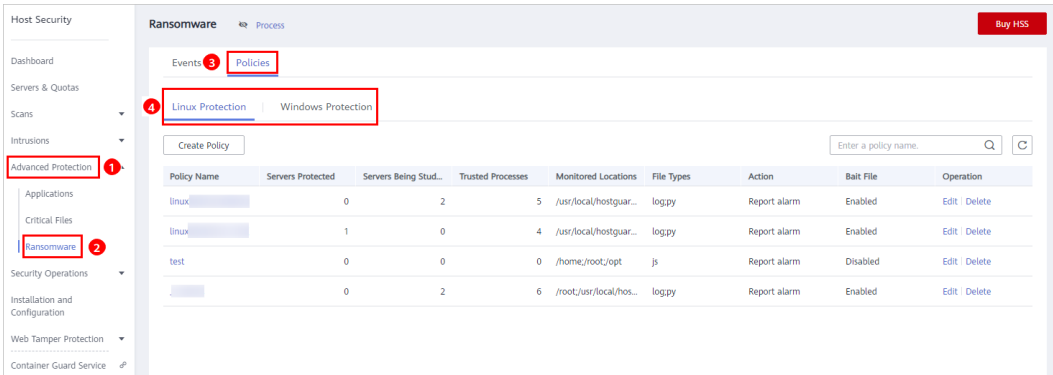


Table 8-9 Policy parameters

Parameter	Description
Policy Name	Policy name
Servers Protected	Number of servers where the policy takes effect
Servers Being Studied	Servers where intelligent learning is in progress. The status of a new policy is **Learning**.
Trusted Processes	Number of trusted processes automatically identified by HSS

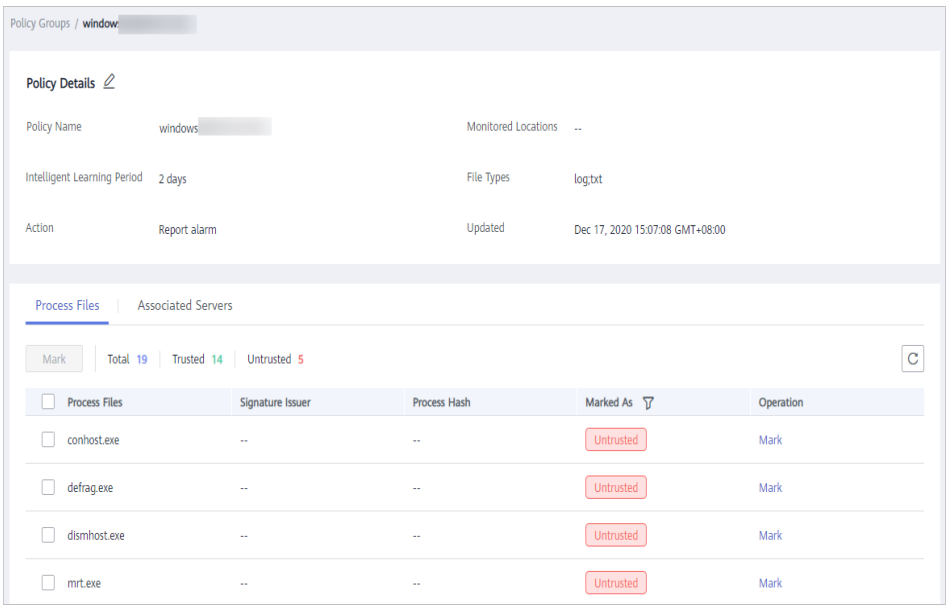
 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Monitored Locations	Path of monitored files. Multiple paths are separated by semicolons (;). Operations on the files in these paths are monitored. If no paths are specified (-- is displayed), all the files on the servers associated to the policy are monitored.
File Types	Extensions of monitored files
Action	Action taken when suspicious operations on monitored files are detected. For example, report alarms.
Bait File	Bait files can be enabled only on Linux servers. • **Enabled**: The bait file function is enabled. HSS puts a bait file on each protected server. Ransomware attempting to encrypt bait files will trigger alarms immediately. • **Disabled**: The bait file function is disabled.

Step 4 Click a policy name to check its details and process files, as shown in **Figure 8-29**.

- You can check the policy name, intelligent learning period, protection status, monitored file path, file name extension, and update time.
- You can check the total number of processes, number of trusted processes, number of untrusted processes, process files, signature issuer, process hash, and trust status.
- You can mark a process file as **Trusted** or **Untrusted**. An untrusted policy can be alarmed based on the policy you set.

Figure 8-29 Protection policy details



Step 5 Click **Associated Servers** to check servers associated to the policy, as shown in **Figure 8-30**.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-30 Checking associated servers

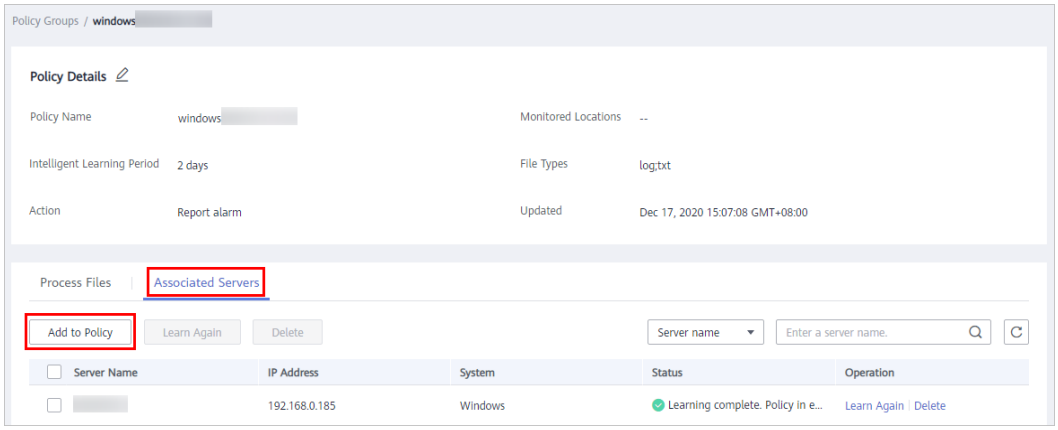


Table 8-10 Associated servers

Parameter	Description
Server Name	Server name
IP Address	Server IP address
System	Server OS. Only Windows OSs can be protected.
Status	Policy status. Its value can be: ● Learning Intelligent learning is in progress. After a policy is created, the intelligent learning function automatically analyzes operations on associated servers. The status of a new policy is **Learning**. ● Learning complete. Policy in effect Intelligent learning is complete. The policy has taken effect on associated servers.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Operation	Operations that can be performed on the policy, including: ● Learn Again – If any software you use was greatly modified, learning must be performed again on associated servers. Click **Learn Again**. – If intelligent learning period you set is too short, learning results will be inaccurate. If the learning still continuous after the period expires, the policy status will remain **Learning**. In these cases, set **Intelligent Learning Period** to a proper duration and click **Learn Again**. – If the server is in **Stopped** or **Faulty** state, the agent is in **Offline** state, or the premium edition is disabled during learning, learning will be interrupted. The policy status will still be **Learning**, but the system will not respond if you click **Learn Again**. In this case, ensure the server is in **Running** state, the agent is in **Online** state, and the premium edition is enabled for the server, and click **Learn Again**. ● Delete Removes an associated server. Files on the server will no longer be protected by the policy.

----End

Editing a Protection Policy

If a protection policy is edited, intelligent learning will be performed based on the new policy settings.

If you disable the bait file function in a policy, the bait files created for the policy will be deleted and HSS will be unable to trap and kill ransomware. Exercise caution when performing this operation.

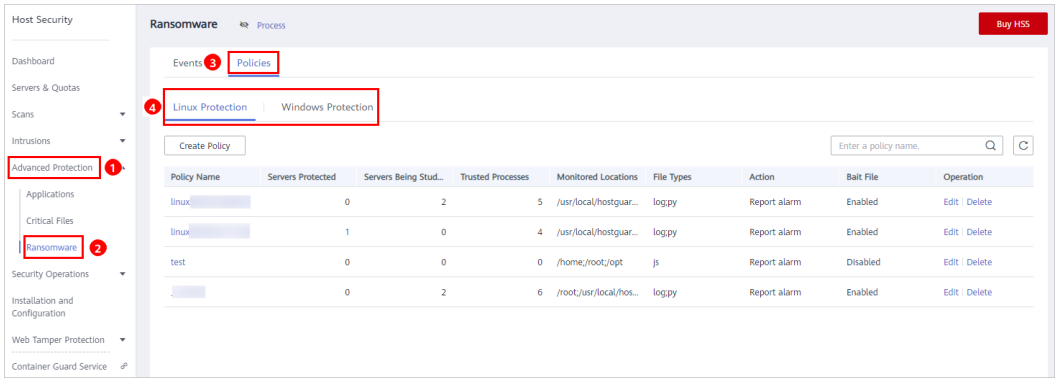
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Ransomware** page, click the **Policies** tab. The ransomware prevention policy list is displayed, as shown in **Figure 8-28**.

 Copyright © Huawei Technologies Co., Ltd.

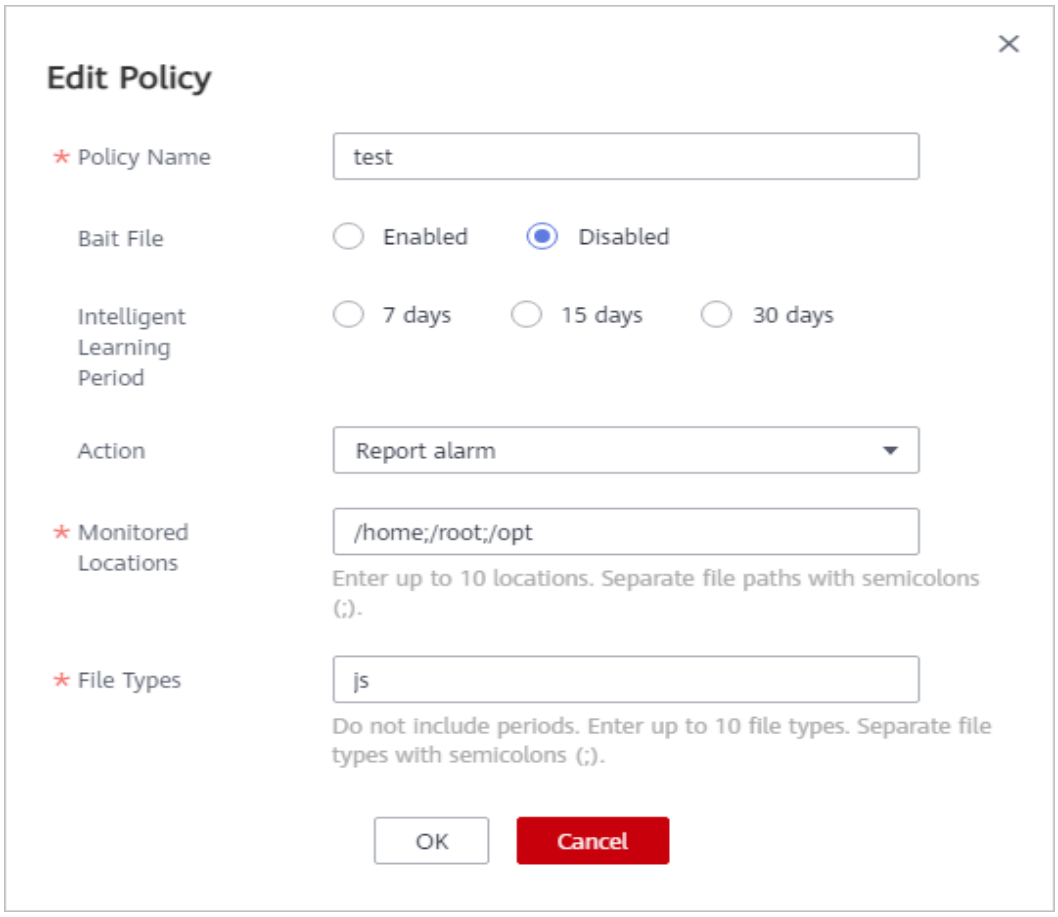
Figure 8-31 Policy list



Step 4 Click **Edit**.

You can modify the policy name, bait file setting, intelligent learning period, protection status, monitored file paths, and file extensions.

Figure 8-32 Editing a policy



Step 5 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Managing Associated Servers in a Policy

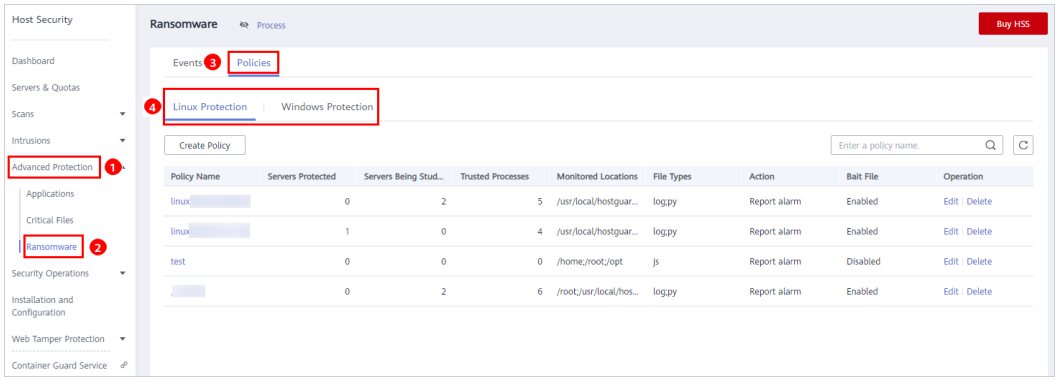
You can associated servers to an existing intelligent learning policy on the **Associated Servers** tab on the policy details page.

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

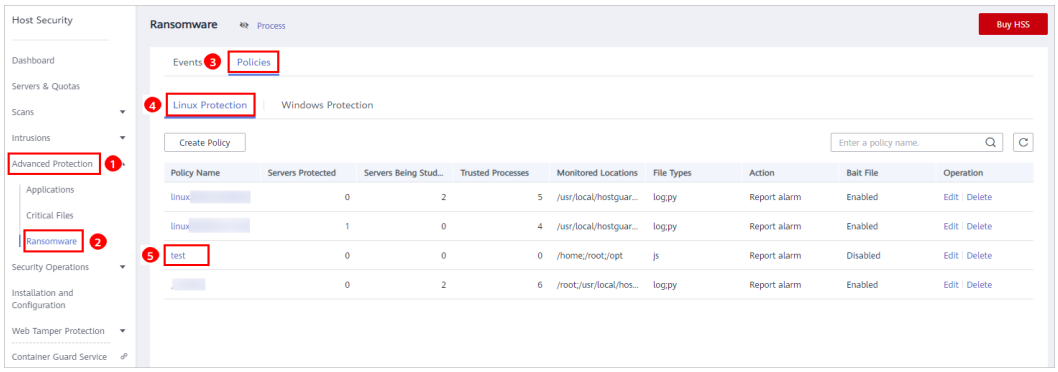
Step 3 On the **Ransomware** page, click the **Policies** tab. The ransomware prevention policy list is displayed, as shown in **Figure 8-28**.

Figure 8-33 Policy list



Step 4 Click the name of a policy. **Figure 8-34** illustrates how to select a Linux policy as an example.

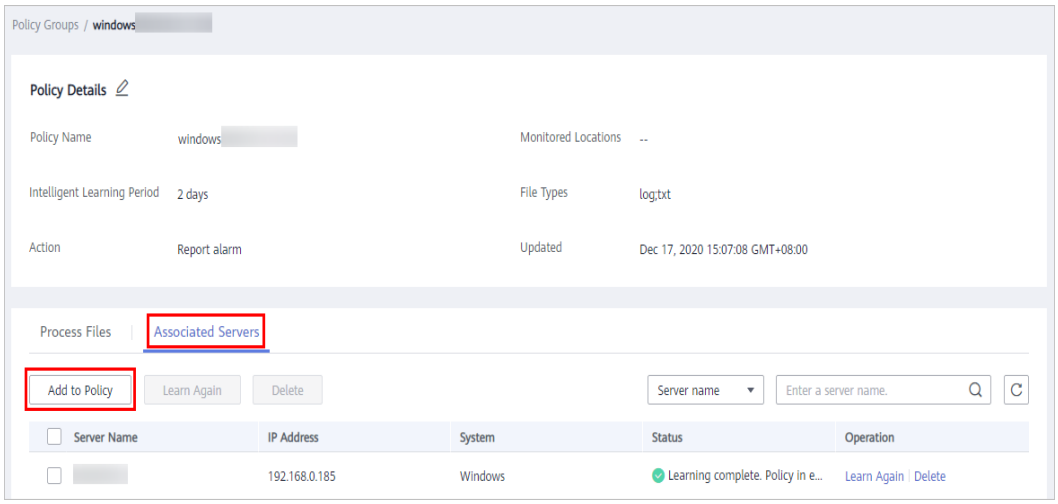
Figure 8-34 Accessing the policy details page



Step 5 Click the **Associated Servers** tab and click **Add Server**, as shown in **Figure 8-35**.

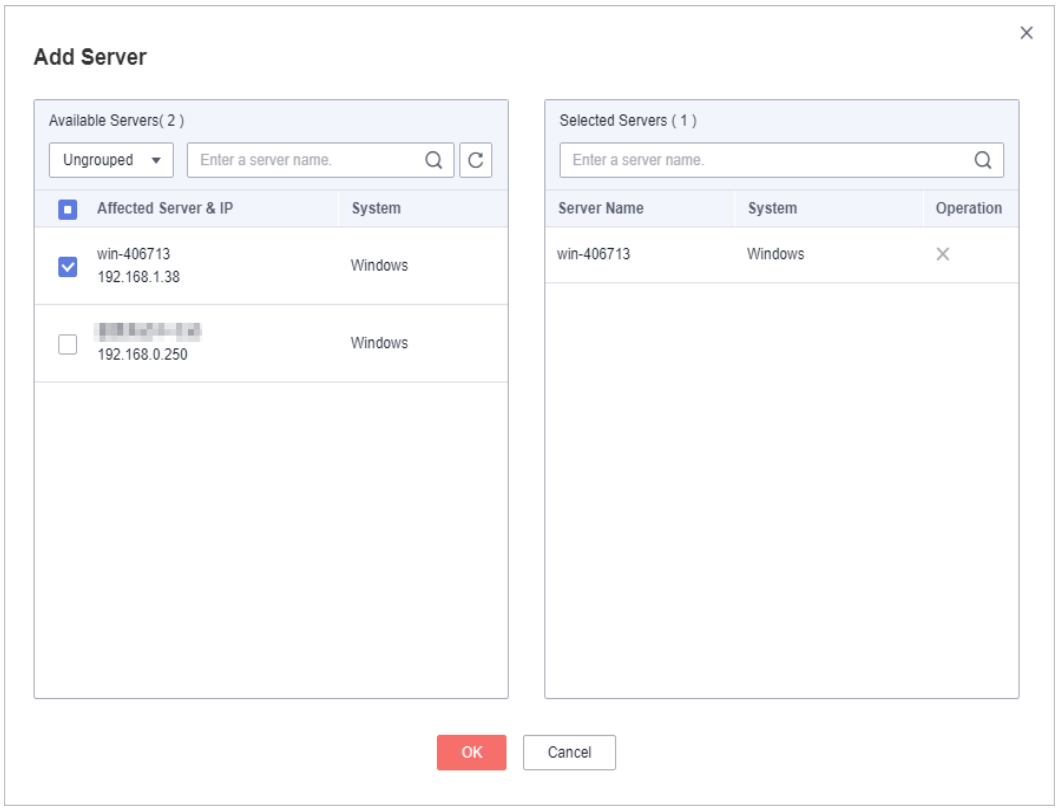
 Copyright © Huawei Technologies Co., Ltd.

Figure 8-35 Adding associated servers



Step 6 In the displayed **Add Server** dialog box, select servers, as shown in **Figure 8-36**.

Figure 8-36 Associating Windows servers



Step 7 Click **OK**.

After associated servers are added, you can check their server names, IP addresses, systems, and policy. By default, the initial policy status is **Learning**.

After the learning is complete, the policy status changes to **Learning complete. Policy in effect**. The ransomware prevention policy will automatically take effect on all servers associated with it.

----End

 Copyright © Huawei Technologies Co., Ltd.

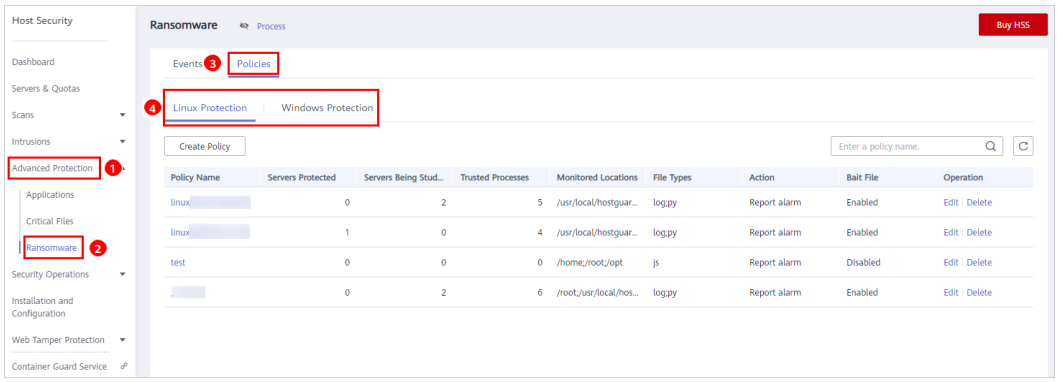
Deleting a Protection Policy

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Ransomware** page, click the **Policies** tab. The ransomware prevention policy list is displayed, as shown in **Figure 8-28**.

Figure 8-37 Policy list



Step 4 Click **Delete**.

Step 5 Click **OK**. After a policy is deleted, the applications on the servers associated to it will no longer be protected.

----End

8.3.4 Handling an Alarm Event

If a ransomware protection policy takes effect on servers, HSS will check operations performed on monitored files on the servers, mark the operations as trusted or untrusted, and report alarms on operations performed by the applications that are untrusted or not specified in the policy.

The event management page displays untrusted operations that match a policy and the operations performed by applications that are not specified in any policies.

You should manually check untrusted events and prevent them from harming your servers.

NOTE

You are advised to pay attention to these events and handle them in a timely manner.

Ransomware prevention is a trial function in the current version. To use stronger functions, purchase HSS (New).

Checking the Alarm Event List

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

 Copyright © Huawei Technologies Co., Ltd.

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Ransomware** page, click the **Events** tab, as shown in **Figure 8-38**.

Figure 8-38 Ransomware prevention events

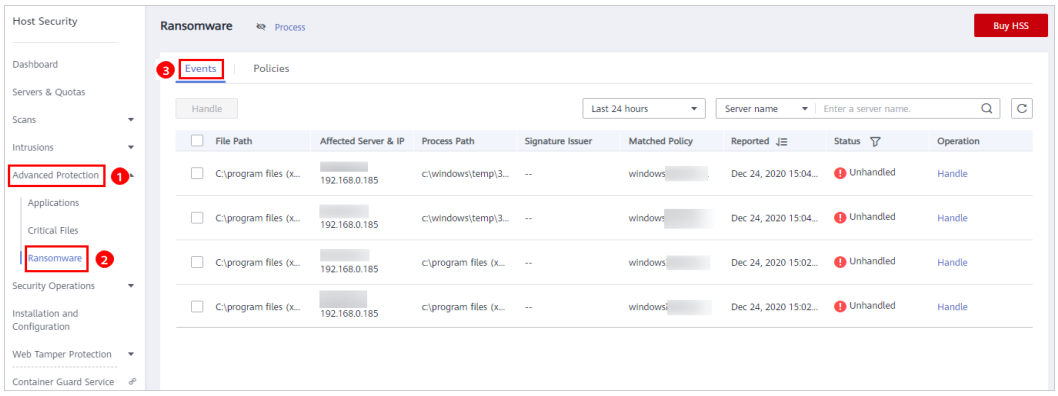


Table 8-11 Ransomware prevention event parameters

Parameter	Description
File Path	Path of the file operated by an application
Affected Server & IP	Name and IP address of the server where the file operation is performed
Process Path	Path of the Application that performs operations on files
Signature Issuer	Signature issuer
Matched Policy	Policy that matches the alarm
Reported	Time when an alarm is reported
Status	Event status. Its value can be **Handled** or **Unhandled**.

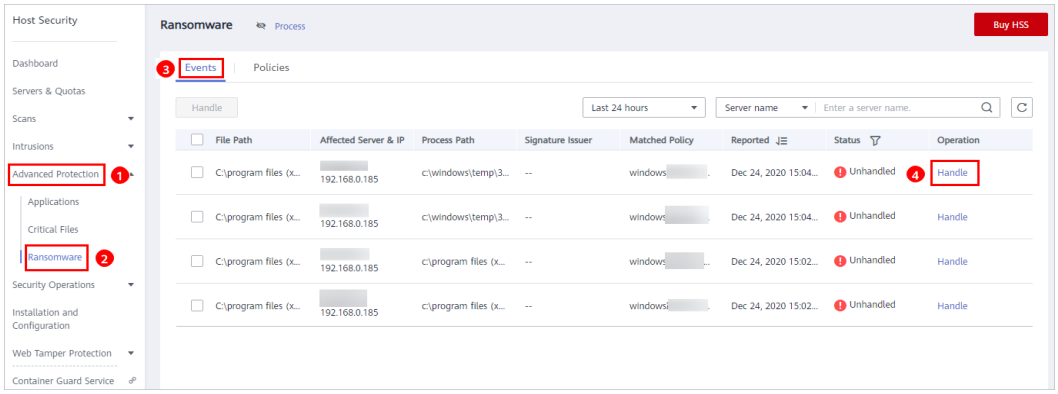
----End

Handling an Alarm Event

Step 1 In the **Operation** column of an event, click **Handle**, as shown in **Figure 8-39**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-39 Checking ransomware prevention events



Step 2 In the displayed dialog box, select **Trusted** or **Untrusted**, as shown in **Figure 8-40**.

Figure 8-40 Handling ransomware events

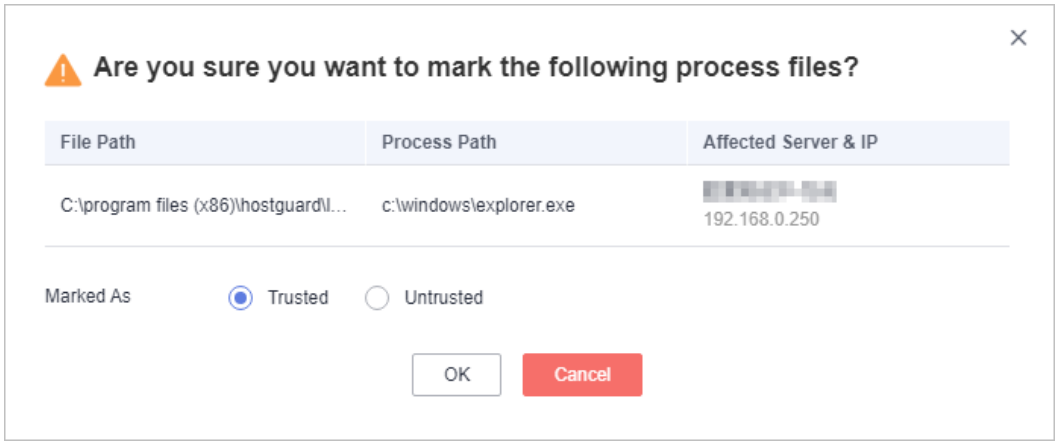


Table 8-12 Event handling parameters

Marked As	Description
Trusted	An application marked as trusted will not trigger alarms if it performs operation on files under monitored paths.
Untrusted	An application marked as untrusted will trigger alarms if it performs operation on files under monitored paths.

Step 3 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

9 Security Operations

9.1 Checking or Creating a Policy Group

You can group policies and servers to batch apply policies to servers, easily adapting to business scenarios.

Precautions

- When you enable the enterprise edition, the default policy group of this edition (including weak password and website shell detection policies) takes effect for all your servers.
- When you enable the premium edition you separately purchased or included with the WTP edition, the default policy group of this edition takes effect.

  To create your own policy group, you can copy the default policy group and add or remove policies in the copy.

Policy List

Policy	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition
Weak Password Scan	Change weak passwords to stronger ones based on HSS scan results and suggestions.	Linux and Windows	√ (Check only custom weak passwords)	√	√
Web Shell Scan	Scan web directories on servers for web shells.	Linux and Windows	√ (Check only specified paths)	√	√

 Copyright © Huawei Technologies Co., Ltd.

Policy	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition
Assets	Scan and display all software in one place, including software name, path, and major applications, helping you identify abnormal assets.	Linux and Windows	×	√	√
System Settings Scan	Check for unsafe Tomcat, Nginx, and SSH login configurations.	Linux and Windows	×	√	√
High-risk Command Scan	Check executed commands in real time and generate alarms if high-risk commands are detected.	Linux	×	√	√
Privilege Escalation Scan	Detect privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities ● File privilege escalation	Linux	×	√	√

Copyright © Huawei Technologies Co., Ltd.

Policy	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition
Abnormal Shell Scan	Detect actions on abnormal or reverse shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	Linux	×	√	√
File Integrity Monitoring	Check the files in the Linux OS, applications, and other components to detect tampering.	Linux	×	√	√

Accessing the Policies Page

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Security Operations** > **Policies**.

----End

Checking the Policy Group List

Step 1 Go to the **Policies Groups** page, as shown in **Figure 9-1**. For more information, see **Table 9-1**.

NOTE

- **default_enterprise_policy_group** is the default policy group of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted.
- **default_premium_policy_group** is the default policy group of the premium edition. You can create a policy group by copying this default group and modify the copy.
- To refresh the list, click  in the upper right corner.
- To view details about the servers associated with a policy group, click the number in the **Servers** column of the group.

Figure 9-1 Policy group list

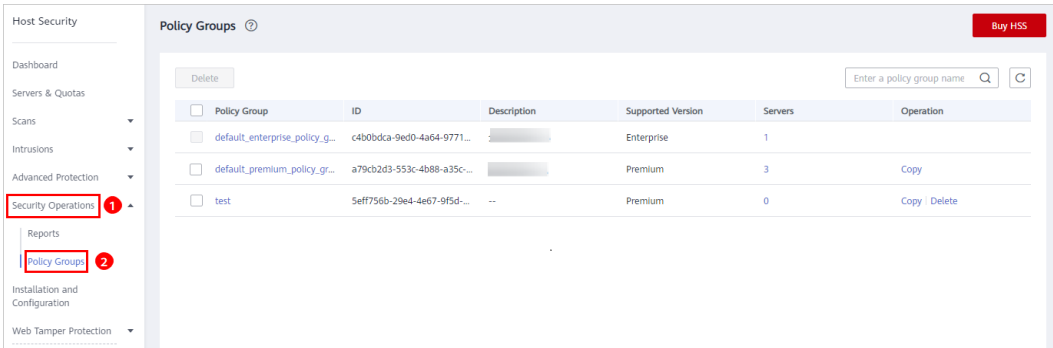


Table 9-1 Policy group parameters

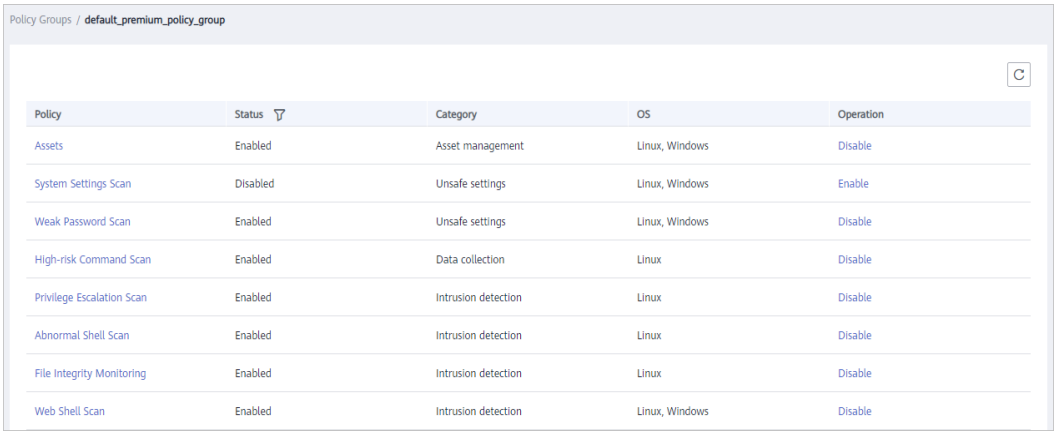
Parameter	Description
Policy Group Name	Name of a policy group
ID	Unique ID of a policy group
Description	Description of a policy group
Supported Version	HSS edition supported by a policy group

Step 2 Click the name of a policy group to check policy details, including the names, statuses, function categories, OS type of the policies, as shown in **Figure 9-2**.

NOTE

- By default, all policies in the groups **default_enterprise_policy_group** and **default_premium_policy_group** are enabled.
- You can click **Enable** or **Disable** in the **Operation** column of a policy to control what to check.

Figure 9-2 Policy group details



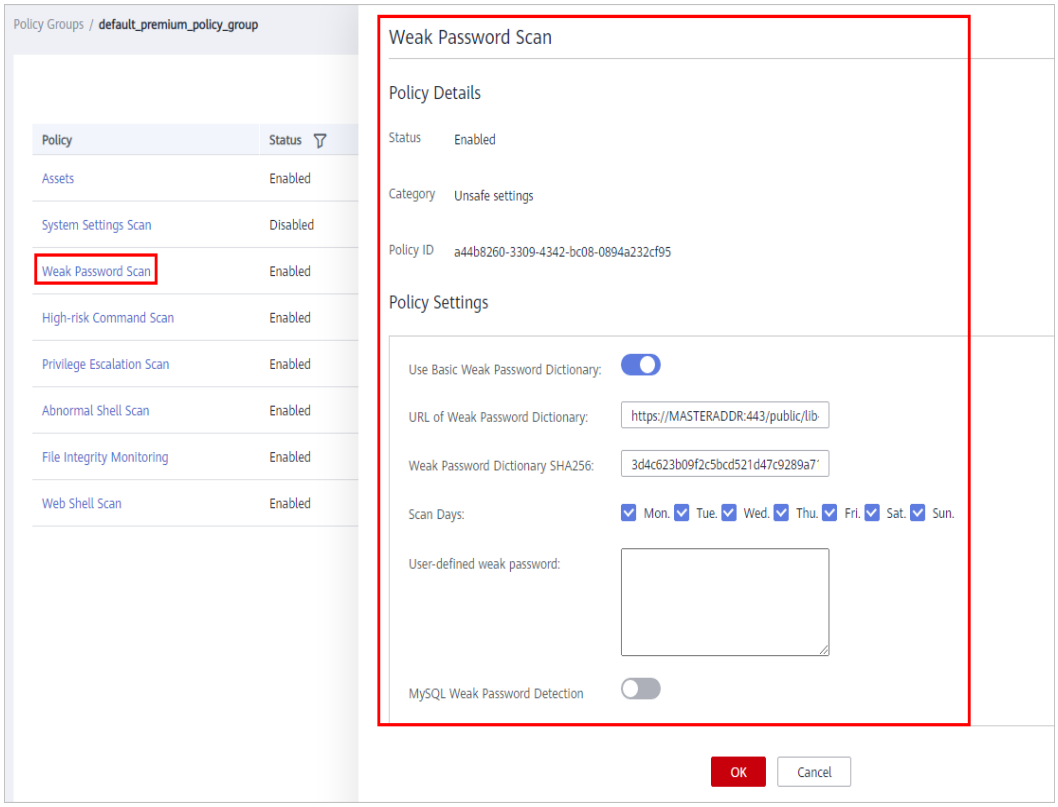
Step 3 Click the name of a policy to check its details. **Figure 9-3** shows the **Weak Password Scan** policy as an example.

Copyright © Huawei Technologies Co., Ltd.

NOTE

For details about how to modify a policy, see **Modifying a Policy**.

Figure 9-3 Policy details

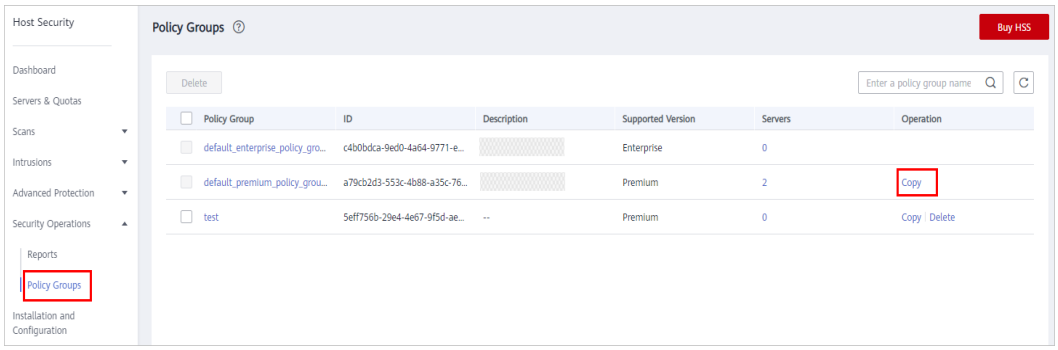


----End

Creating a Policy Group

Step 1 In the row where **default_premium_policy_group (default policy group of the premium edition)** resides, click **Copy** in the **Operation** column, as shown in **Figure 9-4**.

Figure 9-4 Copying a policy group



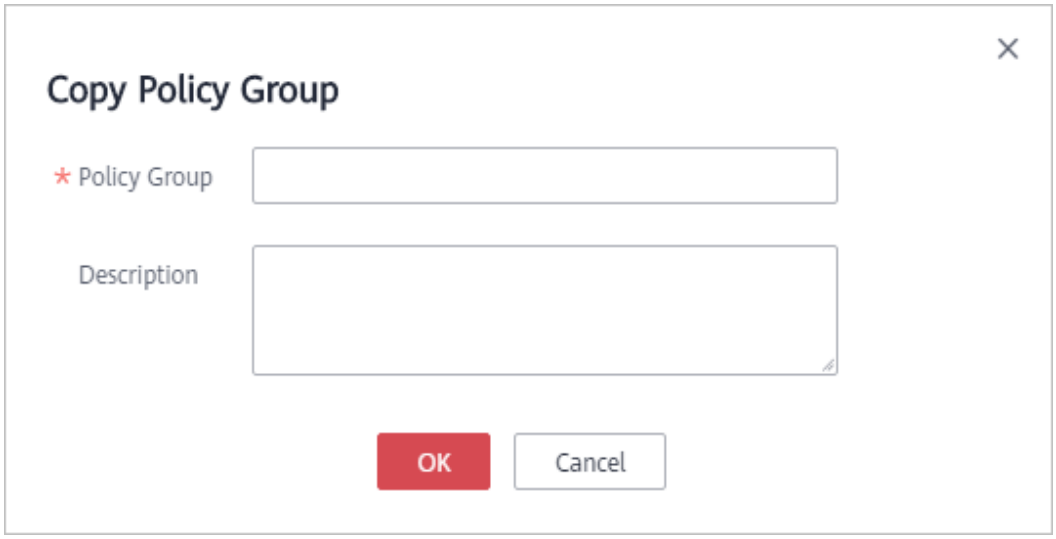
Step 2 In the dialog box displayed, enter a policy group name and description, and click **OK**, as shown in **Figure 9-5**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The name of a policy group must be unique, or the group will fail to be created.
- The policy group name and its description can contain only letters, digits, underscores (_), hyphens (-), and spaces, and cannot start or end with a space.

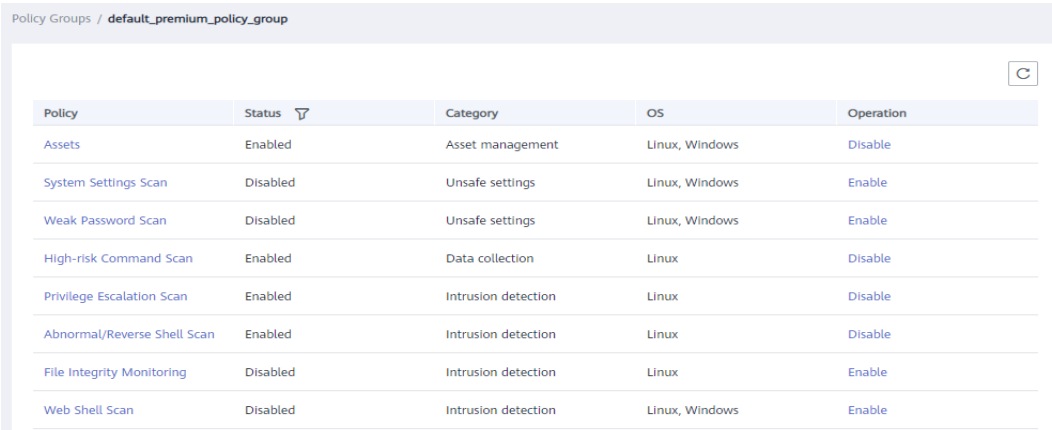
Figure 9-5 Creating a policy group



Step 3 Click **OK**.

Step 4 Click the name of the policy group you just created. The policies in the group will be displayed, as shown in **Figure 9-6**.

Figure 9-6 Policies in a group



Policy	Status	Category	OS	Operation
Assets	Enabled	Asset management	Linux, Windows	Disable
System Settings Scan	Disabled	Unsafe settings	Linux, Windows	Enable
Weak Password Scan	Disabled	Unsafe settings	Linux, Windows	Enable
High-risk Command Scan	Enabled	Data collection	Linux	Disable
Privilege Escalation Scan	Enabled	Intrusion detection	Linux	Disable
Abnormal/Reverse Shell Scan	Enabled	Intrusion detection	Linux	Disable
File Integrity Monitoring	Disabled	Intrusion detection	Linux	Enable
Web Shell Scan	Disabled	Intrusion detection	Linux, Windows	Enable

Step 5 Click a policy name and modify its settings as required. For details, see **Modifying a Policy**.

Step 6 Enable or disable the policy by clicking the corresponding button in the **Operation** column.

----End

 Copyright © Huawei Technologies Co., Ltd.

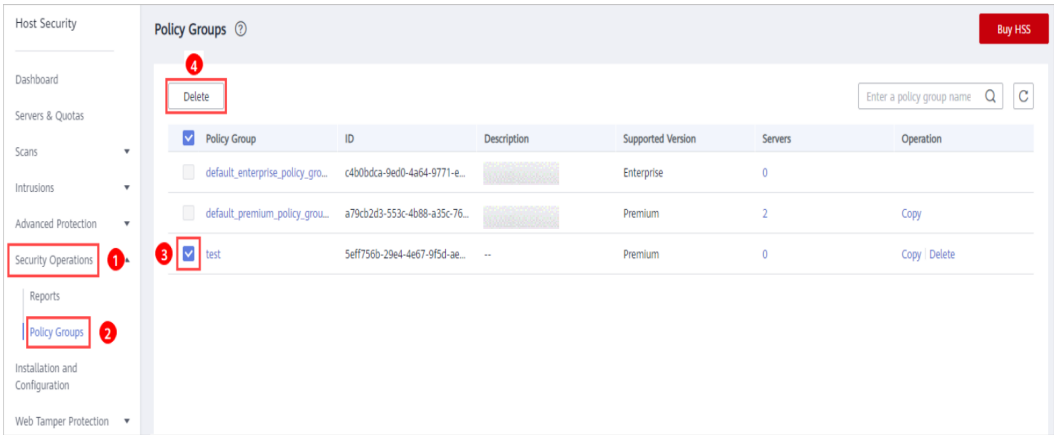
Follow-Up Procedure

Deleting a policy group

After a policy group is deleted, the **Policy Group** column of the servers that were associated with the group will be blank.

Step 1 Select one or more policy groups to be deleted and click **Delete**, as shown in Figure 9-7.

Figure 9-7 Deleting policy groups



NOTE

You can also click **Delete** in the **Operation** column of a policy group to delete it.

Step 2 In the displayed dialog box, click **OK**.

----End

9.2 Modifying a Policy

You can modify policies in a policy group.

NOTICE

Modifications on a policy take effect only in the group it belongs to.

Accessing the Policies Page

Step 1 Log in to the management console.

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Security Operations** > **Policies**.

----End

Copyright © Huawei Technologies Co., Ltd.

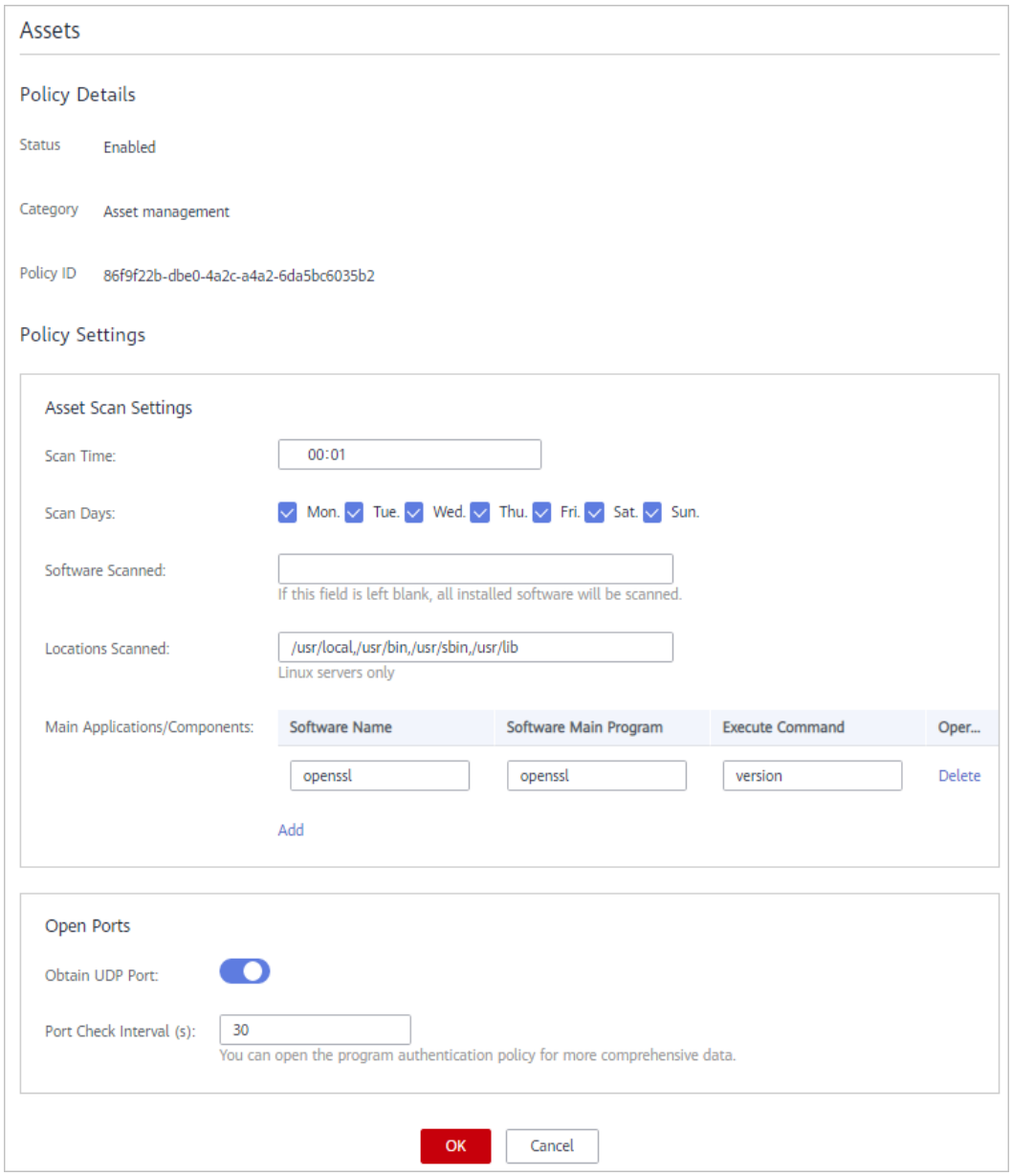
Assets

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **Assets**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 9-8**. For more information, see **Table 9-2**.

Figure 9-8 Assets



 Copyright © Huawei Technologies Co., Ltd.

Table 9-2 Assets parameters

Parameter	Description
Scan Time	Time point when scans are performed. It can be accurate to the minute.
Scan Days	Days in a week when assets are scanned. You can select one or more days.
Software Scanned	• Software name. A name can contain a maximum of 5000 characters without any space. Use commas (,) to separate software names. • If this parameter is not specified, information about all installed software will be retrieved as its value.
Locations Scanned	Software search path. This parameter is not required for a Windows server.
Main Applications/ Components	• **Software Name** • **Software Main Program** • **Execute Command** • **Operation**: You can click **Add** or **Remove** to modify operations.
Obtain UDP Port	Obtains UDP port information and check the web directories. • : enable • : disable
Port Information Check Interval (s)	Interval between two consecutive port checks. The value range is 30s to 86,400s.

Step 4 Click **OK**.

----End

System Configuration Detection

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **System Settings Scan**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 9-9**. For more information, see **Table 9-3**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-9 System settings scan

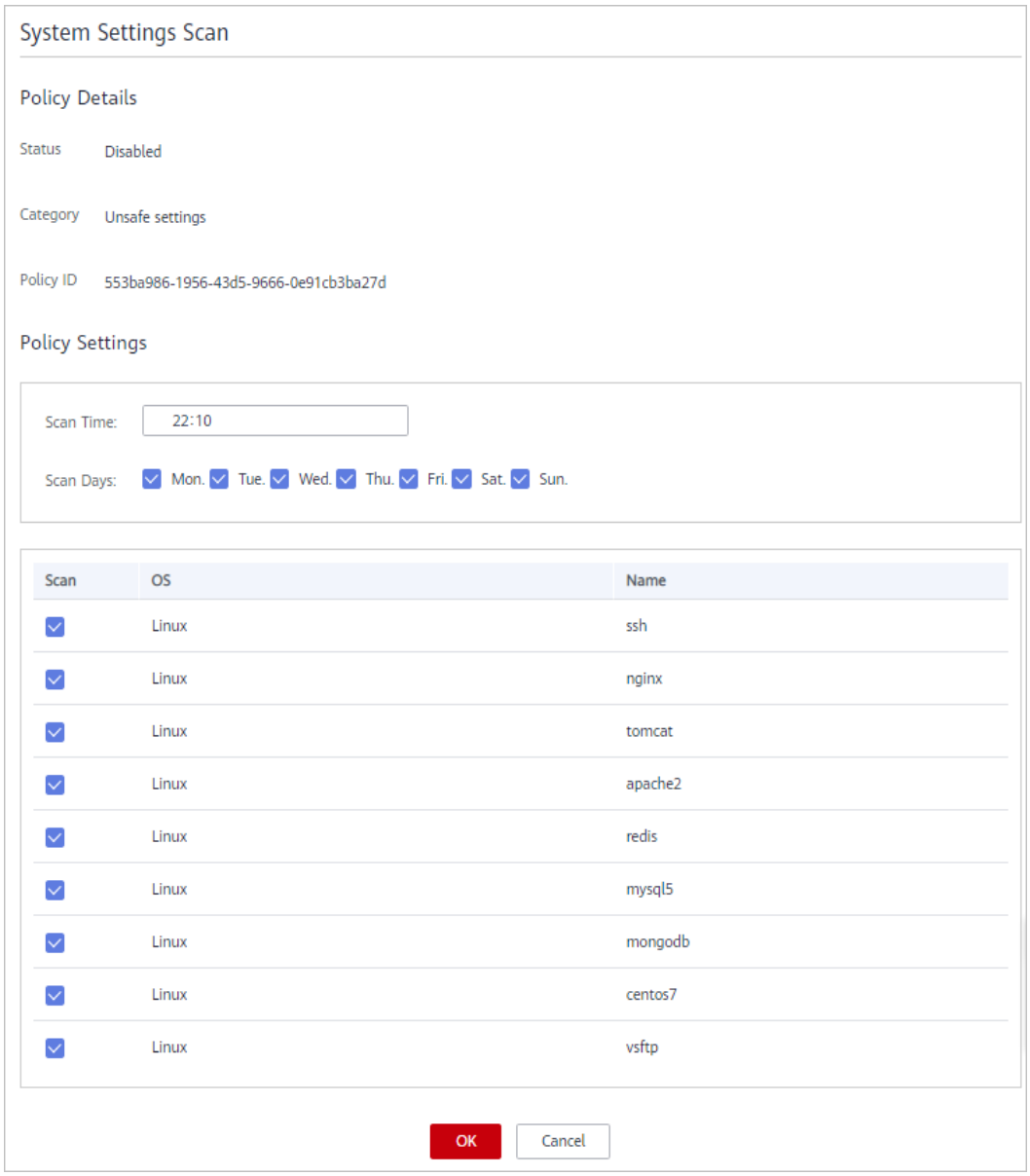


Table 9-3 System settings scan parameters

Parameter	Description
Scan Time	Time point when detections are performed. It can be accurate to the minute.
Scan Days	Day in a week when a detection is performed. You can select any days from Monday to Sunday.

Step 4 Select the OSs to be checked.

Step 5 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Weak Password Scan

Weak passwords are not attributed to a certain type of vulnerabilities, but they bring no less security risks than any type of vulnerabilities. Data and programs will become insecure if their passwords are cracked.

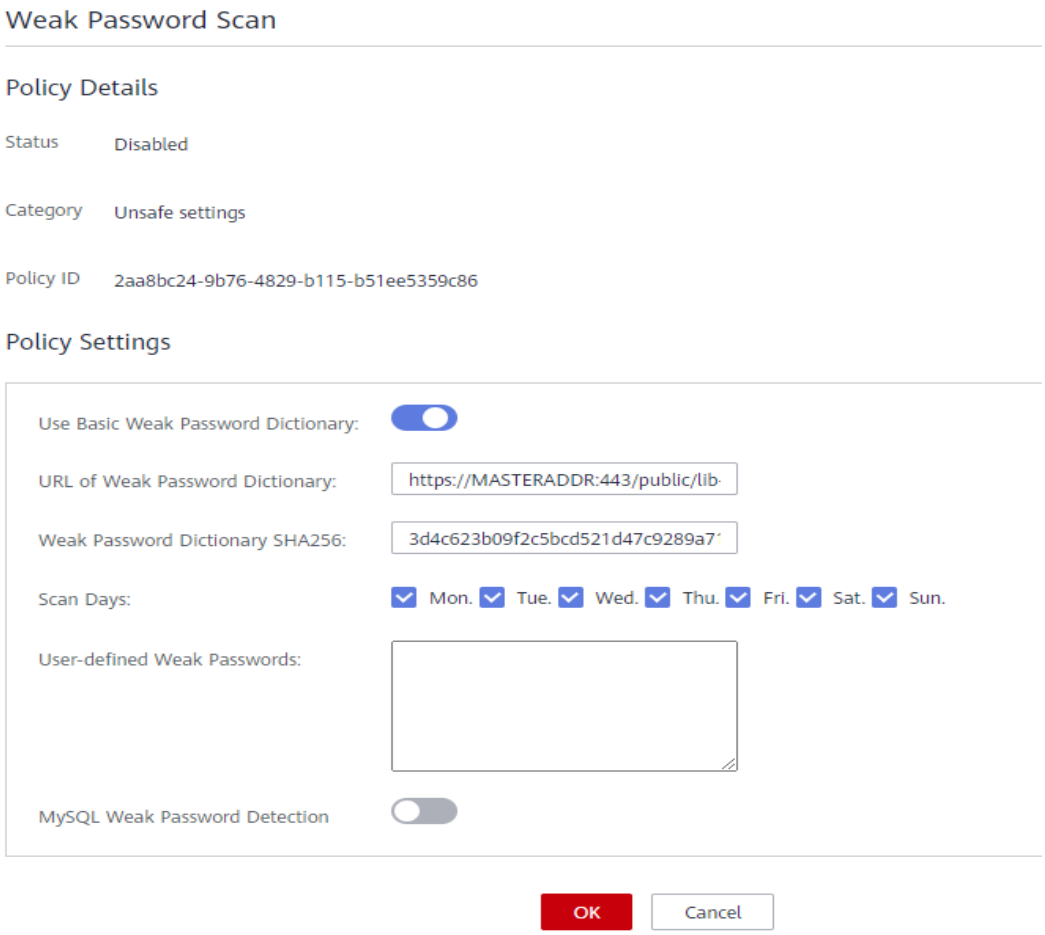
HSS proactively detects the accounts using weak passwords and generates alarms for the accounts. You can also add a password that may have been leaked to the weak password list to prevent server accounts from using the password.

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 In the policy group list, click **Weak Password Scan**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 9-10**. For more information, see **Table 9-4**.

Figure 9-10 Weak password scan



Copyright © Huawei Technologies Co., Ltd.

Table 9-4 Weak password scan parameters

Parameter	Description
Use Basic Weak Password Dictionary	Whether to enable the weak password dictionary. • : enable • : disable
URL of Weak Password Dictionary	URL of the website that the weak password dictionary gets updates from
Weak Password Dictionary SHA256	SHA256 of the weak password dictionary
Scan Days	Days in a week when weak passwords are scanned. You can select one or more days.
User-defined Weak Passwords	You can add a password that may have been leaked to this weak password text box to prevent server accounts from using the password.
MySQL Weak Password Detection	Scans MySQL login passwords for weak passwords.

Step 4 Click **OK**.

----End

High-risk Command Detection

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **High-risk Command Scan**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 9-11**. For more information, see **Table 9-5**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-11 High-risk command detection

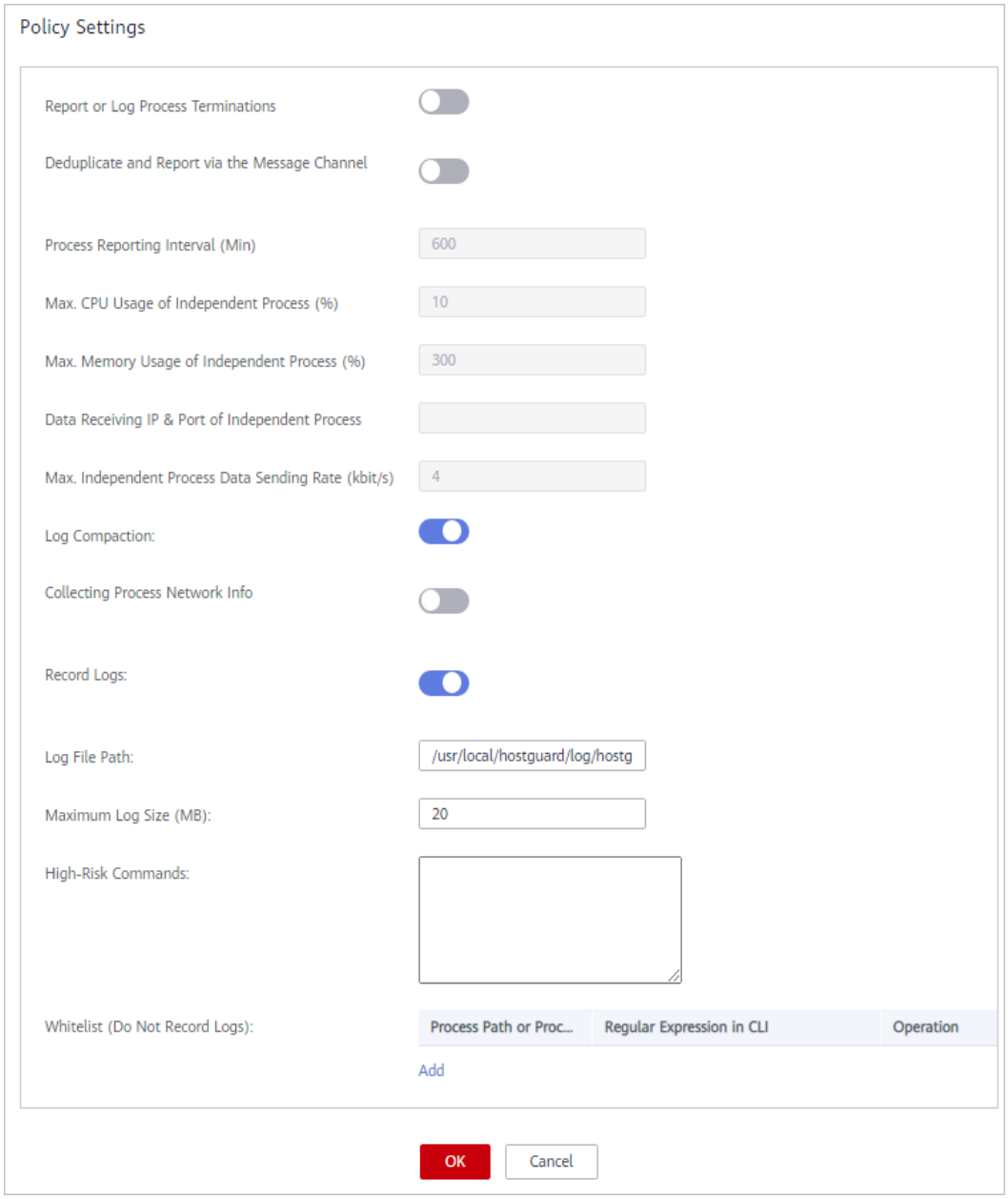


Table 9-5 High-risk command scan parameters

Parameter	Description
Report or Log Process Terminations	Reports or records process termination. • : enable • : disable

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Deduplicate and Report via the Message Channel	De-duplicates messages reported through the message channel. • : enable • : disable
Process Reporting Interval (Min)	This parameter takes effect only if **Deduplicate and Report via the Message Channel** has been enabled. This parameter specifies the interval for reporting process statistics. Set it to a valid number.
Max. CPU Usage of Independent Process (%)	This parameter takes effect only if **Deduplicate and Report via the Message Channel** has been enabled. This parameter specifies the maximum CPU usage of an independent process. The value range is 5 to 99.
Max. Memory Usage of Independent Process (MB)	This parameter takes effect only if **Re-reporting via the Message Channel** has been enabled. This parameter specifies the maximum memory usage of an independent process. The value range is 50 to 1024.
Data Receiving IP & Port of Independent Process	This parameter takes effect only if **Re-reporting via the Message Channel** has been enabled. This parameter specifies the data receiving IP address and port of an independent process.
Max. Independent Process Data Sending Rate (kbit/s)	This parameter takes effect only if **Re-reporting via the Message Channel** has been enabled. This parameter specifies the maximum data sending rate of an independent process. The value range is 1 to 100.
Log Compaction	Compacts logs. • : enable • : disable
Collecting Process Network Info	Collects network connection information of processes. • : enable • : disable
Record Logs	Records logs. • : enable • : disable
Log File Path	Log file path

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Maximum Log Size (MB)	Maximum size of a log file. The value range is 10 to 1024. ● If the size of a .log file exceeds the allowed maximum size, the system automatically renames the file as **.log.0**, creates a new .log file, and writes logs to the .log file. ● A maximum of two log files can exist. If the .log file exceeds the allowed maximum size, the system deletes the **.log.0** file, renames the .log file as **.log.0**, creates a new .log file, and writes logs to the .log file.
High-Risk Commands	High-risk commands you want HSS to detect. Each command occupies a line.
Whitelist (Do Not Record Logs)	● **Process Path or Process Name**: full path of a process or full name of a program ● **Regular Expression in CLI**: regular expression of a command ● **Operation**: You can click **Add** or **Delete** to modify the list of processes and programs.

Step 4 Click **OK**.

----End

Privilege Escalation Scan

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **Privilege Escalation Scan**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 9-12**. For more information, see **Table 9-6**.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-12 Privilege escalation detection

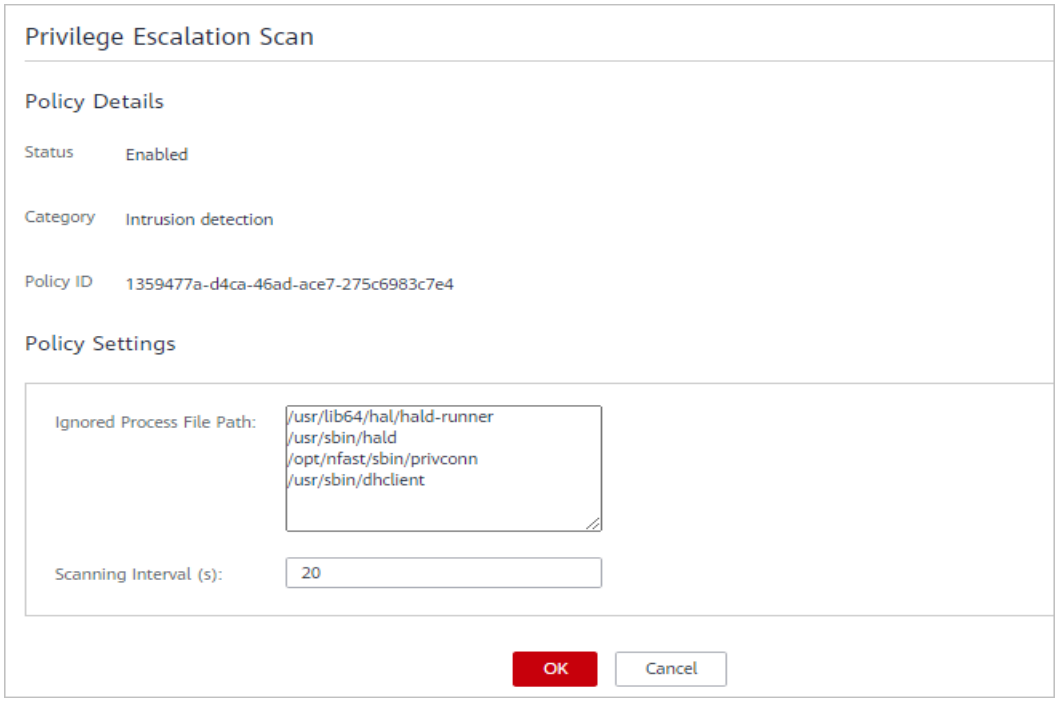


Table 9-6 Privilege escalation scan parameters

Parameter	Description
Ignored Process File Path	Ignored process file path
Scanning Interval (s)	Interval for checking process files. The value range is 5 to 3600.

Step 4 Click **OK**.

----End

Abnormal or Reverse Shell Scan

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **Abnormal/Reverse Shell Scan**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 9-13**. For more information, see **Figure 9-13**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-13 Abnormal or reverse shell scan

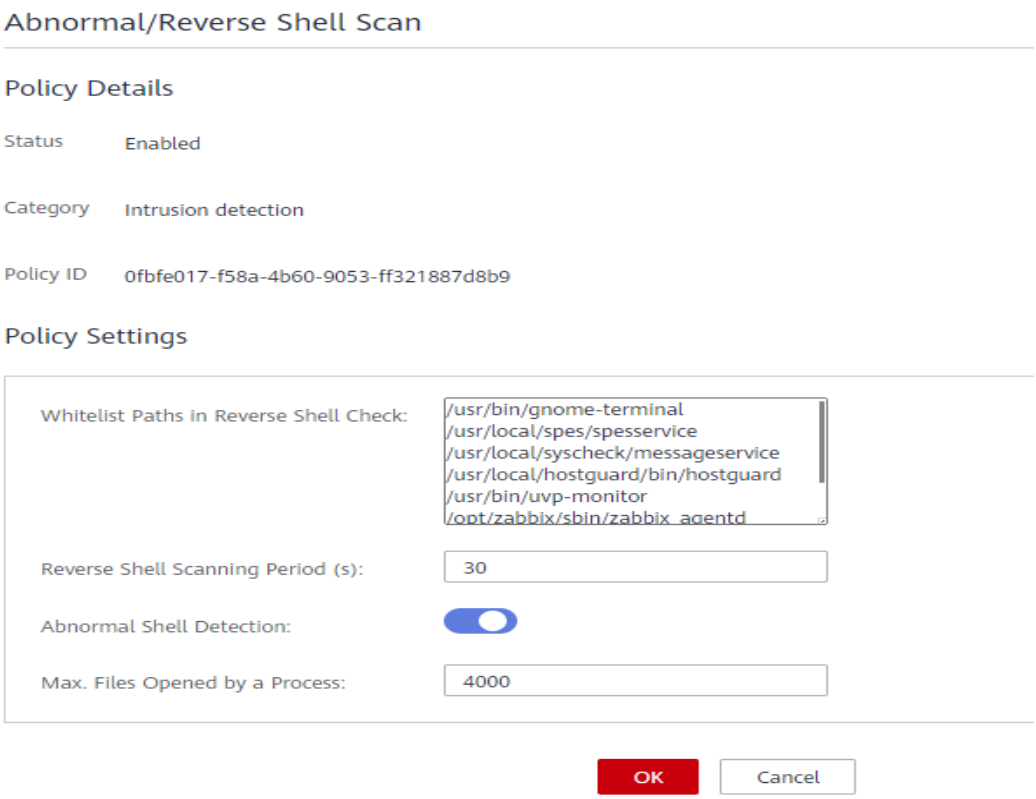


Table 9-7 Abnormal or reverse shell scan parameters

Parameter	Description
Whitelist Paths in Reverse Shell Check	Process file path to be ignored in reverse shell detection
Reverse Shell Scanning Period (s):	Reverse shell scanning period. The value range is 30 to 86,400.
Abnormal Shell Detection	Detects abnormal shells. You are advised to enable it. • : enable • : disable
Max. Files Opened by a Process	Maximum number of files that can be opened by a process. The value range is 10 to 300,000.

Step 4 Click **OK**.

----End

File Integrity Monitoring

Step 1 In the policy group list, click the name of the group that contains the required policy.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Click **File Integrity Monitoring**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 9-14**. For more information, see **Table 9-8**.

Figure 9-14 Integrity check on critical files

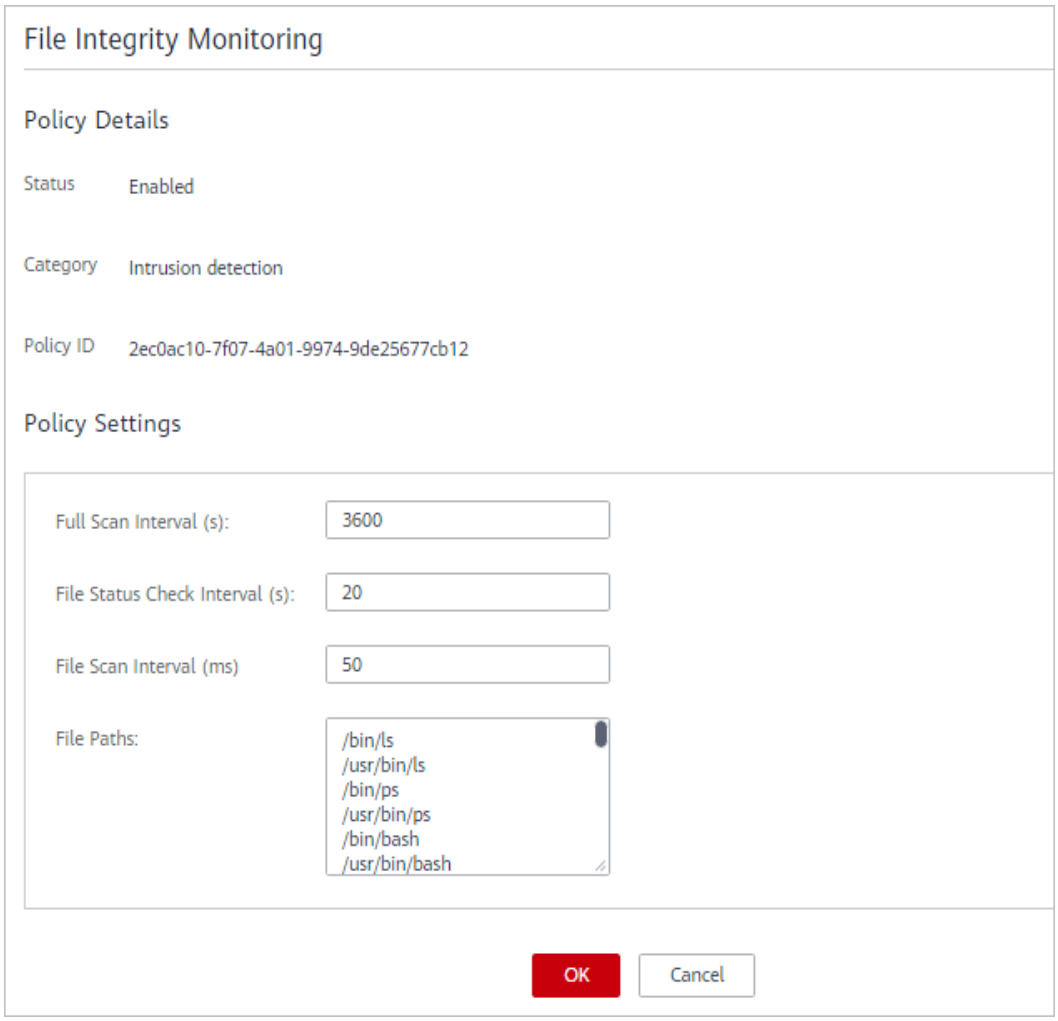


Table 9-8 File integrity monitoring parameters

Parameter	Description
Full Scan Interval (s)	Interval between two consecutive full scans on specified files. The value range is 3600 to 100,000. For example, setting it to **3600** means the full scan is performed every hour.
File Status Check Interval (s)	Interval for checking file status. The value range is 10 to 600.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
File Scan Interval (ms)	Interval between the checks of two files. The value range is 0 to 1000. For example, if this parameter is set to **50**, the system checks **/usr/bin/ls** 50 milliseconds after it checks **/bin/ls**.
File Paths	Path of the files to be checked **NOTE** • Exercise caution when modifying its settings. Its default values are all critical files and you are not advised to delete any of them. • HSS does not monitor changes on the files that are not specified here.

Step 4 Click **OK**.

----End

Web Shell Scan

Web shell scan takes effect only after a web path is set.

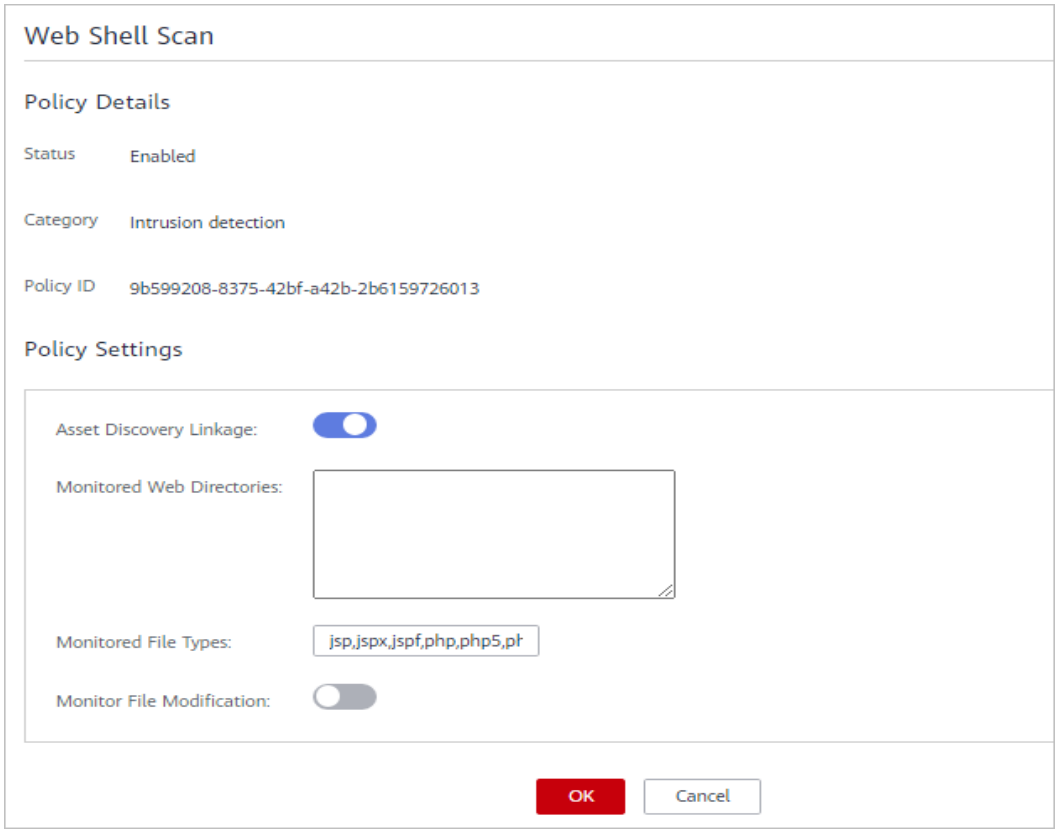
Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **Web Shell Scan**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 9-15**. For more information, see **Table 9-9**.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-15 Web shell scan



NOTE

To prevent the software in web paths from affecting the HSS agent, do not set web paths under **/usr/local**.

Table 9-9 Web shell scan parameters

Parameter	Description
Asset Discovery Linkage	Automatically scans the web paths you specified. • : enable • : disable
Monitored Web Directories	Web paths to be scanned. A file path must: • Start with a slash (/) and end with no slashes (/). • End with a port number. • Occupy a separate line and cannot contain spaces.
Monitored Files Types	Extensions of files to be checked. Valid values include **jsp**, **jspx**, **jspf**, **php**, **php5**, **php4**.
Monitor File Modification	Monitors modifications on files.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Click **OK**.

----End

9.3 Subscribing to HSS Reports

You can subscribe to weekly and monthly reports and check your server security trends, security events, and risks. HSS stores security reports for six months. You are advised to regularly download them to meet certification requirements.

NOTE

- This function is available in Hong Kong, Bangkok, and Singapore regions; and unavailable in Johannesburg, Mexico City 1, Sao Paulo 1, and Santiago regions.
- If you have enabled the enterprise project function, you can select your enterprise project from the **Enterprise project** drop-down list and subscribe to the security report of the project. You can also select **All projects** and subscribe to the security report of servers in all the projects in this region.
- The next day after your subscription, a report of the last subscription period will be generated at 08:00. You can view and download the report.

Downloading an HSS Report

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the HSS console, choose **Security Report**. In the **Operation** column, click **Preview** to view a report.

Figure 9-16 Weekly reports

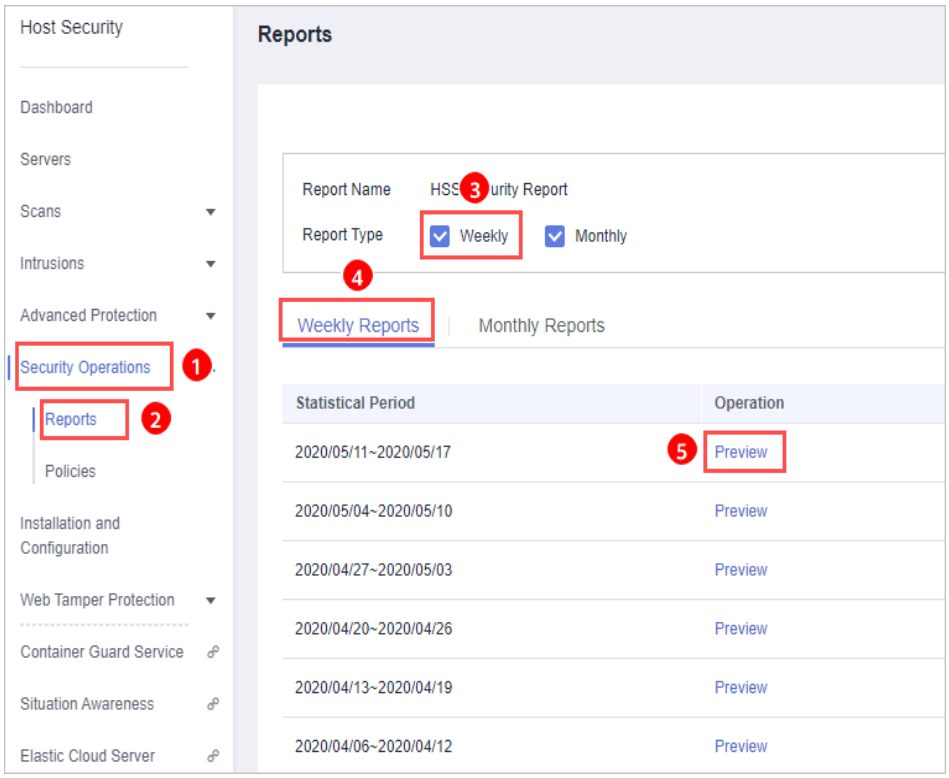
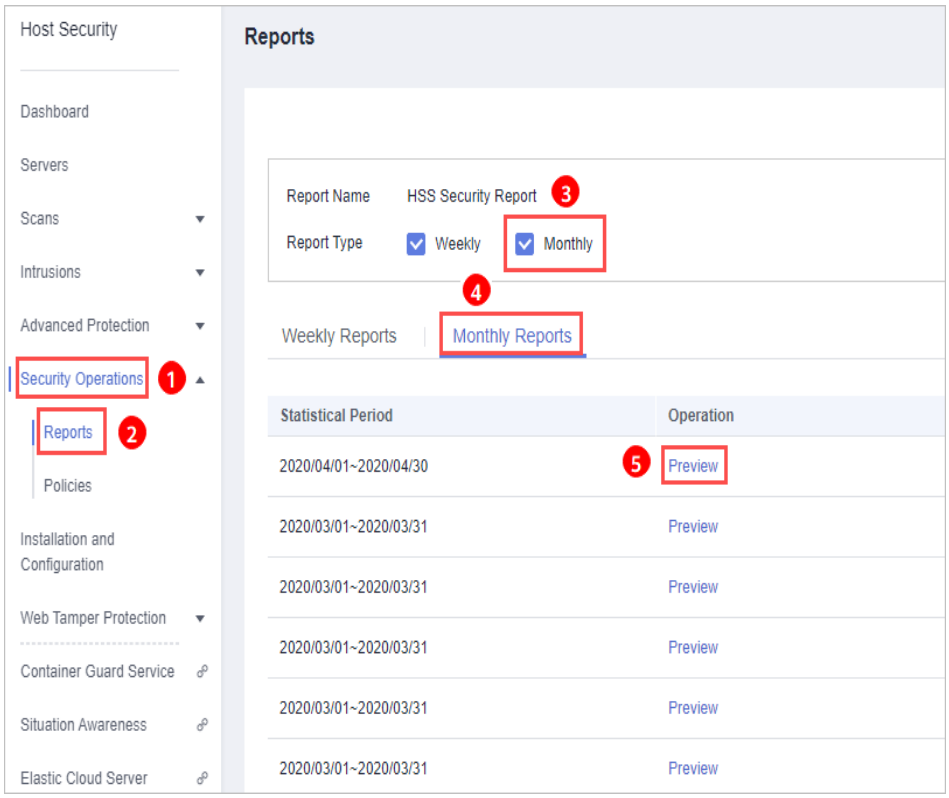


Figure 9-17 Monthly reports



Step 4 Click **Download** on the right of the preview page to download the report.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-18 Downloading a report

----End

HSS Report Template

A weekly or monthly HSS report shows your server security status and helps you handle risks in a timely manner.

A report contains risk overview, risk trend, risk distribution, top 5 high-risk servers, top 5 brute-force attack sources, vulnerability statistics, asset change history, dangerous open ports, weak passwords, unsafe accounts, remote logins, malicious programs, web shells, account cracking attempts, and key file changes.

Take the weekly report template as an example. It contains the following content:

- Risk overview

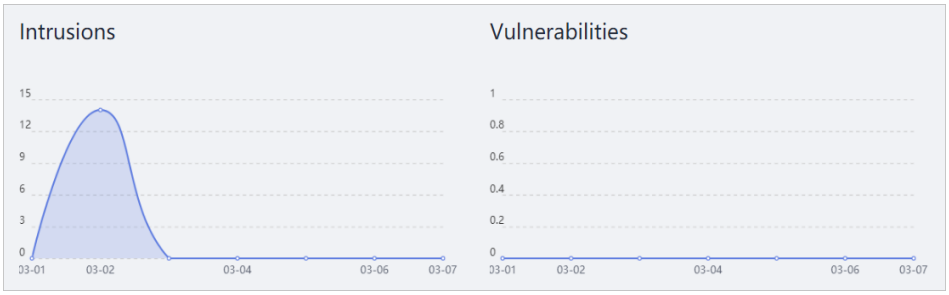
  You can check the risk statistics of this week compared with that of last week.

  Figure 9-19 Risk overview

- Risk trend

  You can check the intrusion and vulnerability trend in the past week.

  Figure 9-20 Risk trend

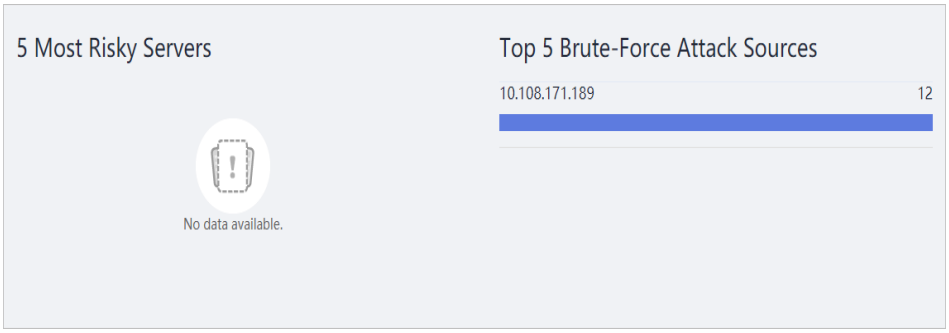


Copyright © Huawei Technologies Co., Ltd.

- Top 5 high-risk servers and top 5 brute-force attack sources

  You can check top 5 high-risk servers and top 5 brute-force attack sources in the past week.

  Figure 9-21 Top 5 high-risk servers and top 5 brute-force attack sources

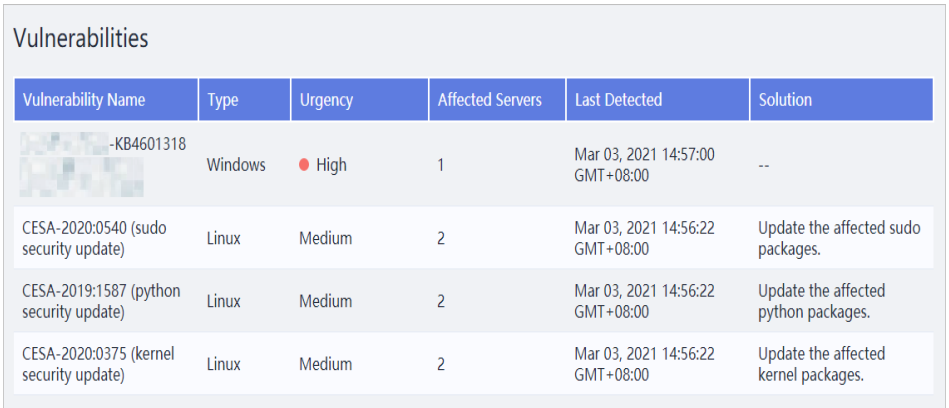


- Vulnerabilities

  You can check vulnerabilities statistics in the past week.

  A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

  Figure 9-22 Vulnerability statistics



Vulnerabilities

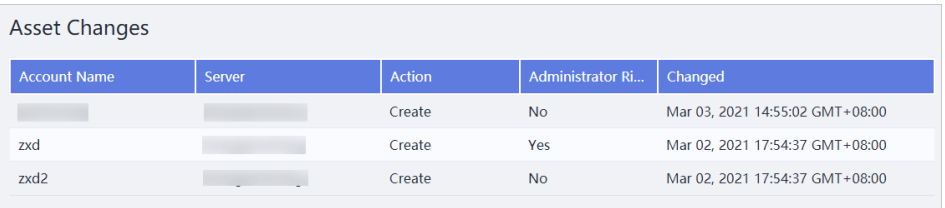
Vulnerability Name	Type	Urgency	Affected Servers	Last Detected	Solution
-KB4601318	Windows	High	1	Mar 03, 2021 14:57:00 GMT+08:00	--
CESA-2020:0540 (sudo security update)	Linux	Medium	2	Mar 03, 2021 14:56:22 GMT+08:00	Update the affected sudo packages.
CESA-2019:1587 (python security update)	Linux	Medium	2	Mar 03, 2021 14:56:22 GMT+08:00	Update the affected python packages.
CESA-2020:0375 (kernel security update)	Linux	Medium	2	Mar 03, 2021 14:56:22 GMT+08:00	Update the affected kernel packages.

- Account changes

  You can check asset changes in the past week.

  A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

  Figure 9-23 Asset changes



Asset Changes

Account Name	Server	Action	Administrator Ri...	Changed
		Create	No	Mar 03, 2021 14:55:02 GMT+08:00
zxd		Create	Yes	Mar 02, 2021 17:54:37 GMT+08:00
zxd2		Create	No	Mar 02, 2021 17:54:37 GMT+08:00

- Unsafe open ports

  You can check unsafe open ports detected in the past week.

Copyright © Huawei Technologies Co., Ltd.

A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

Figure 9-24 Unsafe open ports

High-risk Ports

Local Port	Type	Servers	Risk Level	Status	Description
3388	UDP	1	Unknown	Unhandled	
3388	TCP	1	Unknown	Unhandled	
3390	TCP	1	Unknown	Unhandled	
3390	UDP	1	Unknown	Unhandled	
3391	UDP	1	Unknown	Unhandled	
3391	TCP	1	Unknown	Unhandled	
5050	UDP	1	Unknown	Unhandled	
5353	UDP	1	Unknown	Unhandled	

- Weak passwords

  You can check weak passwords detected in the past week.

  A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

Figure 9-25 Weak passwords

Weak Passwords

Server Name	Account Name	Account Type	Usage Duration (Days)
		System account	0

- Unsafe accounts

  You can check unsafe accounts detected in the past week.

  A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

Figure 9-26 Unsafe accounts

Unsafe Accounts

Account Name	Server	Description	User Group	User Directory	UID/SID	User Startup Shell
			root	/ home/	0	/ bin/ bash

- Remote logins

  You can check the remote logins detected in the past week.

  A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

Figure 9-27 Remote logins

Remote Logins

Server Name	Login Source IP Address	Login Username	Login Time
rasp	.184.191)	root	Mar 03, 2021 16:31:33 GMT+08:00
rasp	.184.191)	root	Mar 03, 2021 16:31:33 GMT+08:00

Copyright © Huawei Technologies Co., Ltd.

- Malicious programs

  You can check the malicious programs detected in the past week.

  A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

  Figure 9-28 Malicious programs

  Malware

Server Name	Program Path	Status	File Per...	User	Program Started	Isolated and Kill...	Description
rasp	/ root/ inotify_x64	Unhandled	--	--	--	--	test

- Web shells

  You can check the web shells detected in the past week.

  A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

  Figure 9-29 Web shells

  Web Shells

Server Name	File Path	Status	Discovered
	/ root/ InsightOpsHandler.php	Unhandled	Mar 03, 2021 15:00:27 GMT+08:00

- Account hacking attempts

  You can check the account hacking attempts detected in the past week.

  A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

  Figure 9-30 Account hacking attempts

  Account Hacking Attempts

Server Name	Attack Source IP ...	Attack Ty...	Blocked ...	Status	First Blocked	Last Blocked
	10.108.171.189	ssh	12	Canceled	Jan 26, 2021 10:31:55 GMT+08:00	Mar 03, 2021 11:41:03 GMT+08:00

- Important file changes

  You can check the important file changes detected in the past week.

  A maximum of 20 risks are listed in the report. For more information, log in to the HSS console.

  Figure 9-31 Important file changes

  Important File Changes

Server Name	Path of Key File	Changed
	/etc/passwd	Mar 03, 2021 14:55:01 GMT+08:00
	/etc/passwd	Mar 03, 2021 14:55:01 GMT+08:00
rasp	/usr/bin/du	Mar 02, 2021 20:42:03 GMT+08:00
rasp	/usr/bin/du	Mar 02, 2021 20:41:17 GMT+08:00
rasp	/usr/bin/du	Mar 02, 2021 20:41:11 GMT+08:00
rasp	/usr/bin/du	Mar 02, 2021 20:36:43 GMT+08:00

Copyright © Huawei Technologies Co., Ltd.

10 WTP

10.1 Adding a Protected Directory

WTP monitors website directories in real time, backs up files, and restores tampered files using the backup, protecting websites from Trojan horses, illegal links, and tampering.

Constraints and Limitations

- WTP only protects files in the protected directories you set. It does not protect the files specified by the links in protected files.
- Ensure the local backup path is valid, or the specified directories will not be protected.
- The local backup path cannot overlap protected directories of the server, or local backup will fail.
- The disk of the local backup path must have sufficient space, or tampering cannot be prevented.

Setting a Protected Directory

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

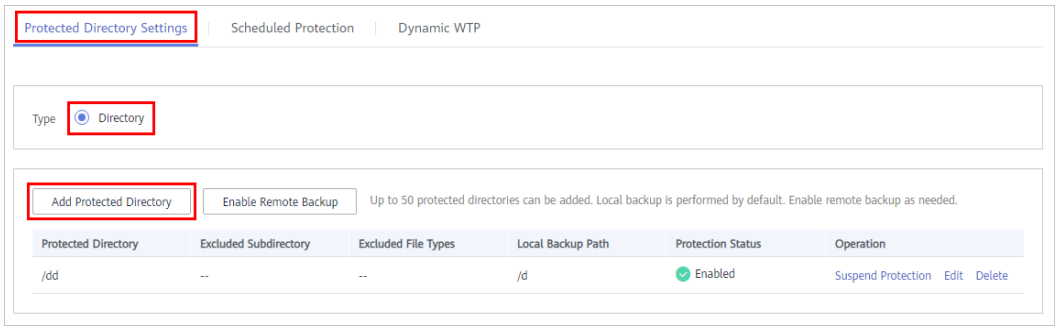
Step 3 Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Step 4 If your server runs the Linux OS, set **Type** to **Directory**, as shown in **Figure 10-1**.

If your server runs the Windows OS, skip this step.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-1 Protecting a specified directory



Step 5 You can add a maximum of 50 protected directories.

1. Click **Add**. In the **Add Protected Directory** dialog box, set required parameters. For details, see **Table 10-1**.

Figure 10-2 Adding a protected directory

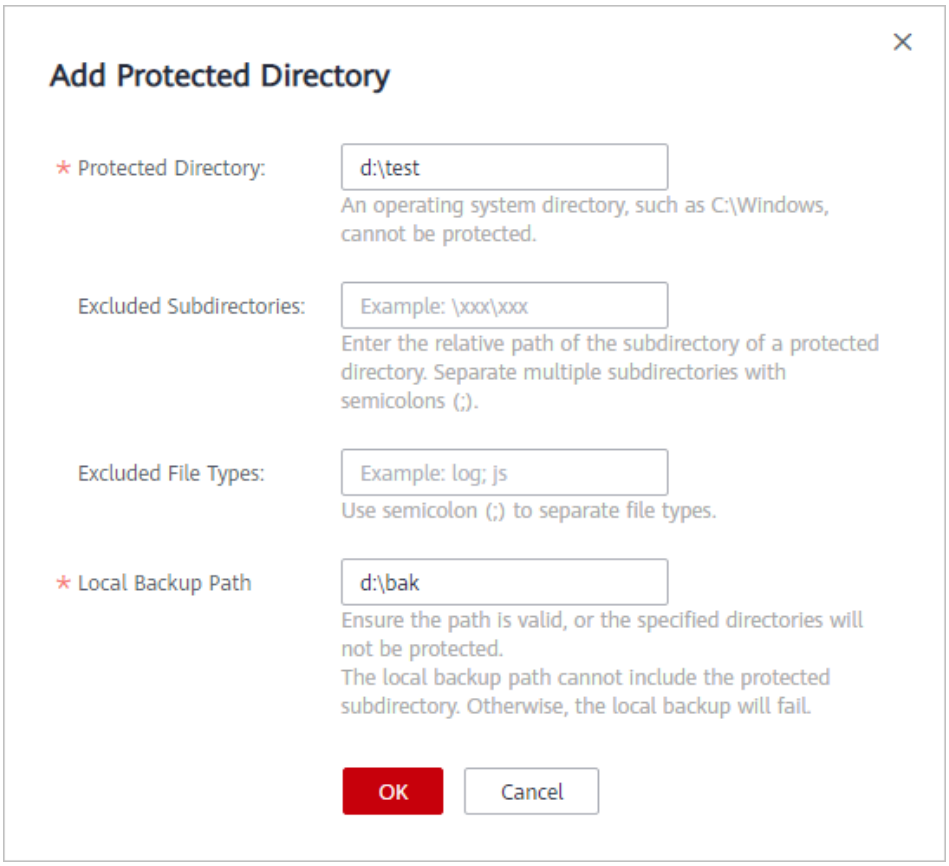


Table 10-1 Parameters for a protected directory

Parameter	Description	Restriction
Protected Directory	Files and folders in this directory are read-only.	Do not set it to any OS directories.

Parameter	Description	Restriction
Excluded Subdirectories	Subdirectories that do not need to be protected in the protected directory, such as temporary file directories. Separate subdirectories with semicolons (;).	The subdirectory is a relative directory in the protected directory.
Excluded File Types	Types of files that do not need to be protected in the protected directory, such as log files. Separate file types with semicolons (;). To record the running status of the server in real time, exclude the log files in the protected directory. You can grant high read and write permissions for log files to prevent attackers from viewing or tampering with the log files.	-
Local Backup Path	After WTP is enabled, files in the protected directory are automatically backed up to the local backup path. Generally, the backup completes within 10 minutes. The actual duration depends on the size of files in the protected directory. Protection takes effect immediately when the backup completes. Excluded subdirectories and types of files are not backed up. If WTP detects that a file in a protected directory is tampered with, it immediately uses the backup file on the local server to restore the file.	The local backup path cannot overlap with the added protected directory.

2. Click **OK**.

   If you need to modify files in the protected directory, stop protection for the protected directory first. After the files are modified, resume protection for the directory in a timely manner.

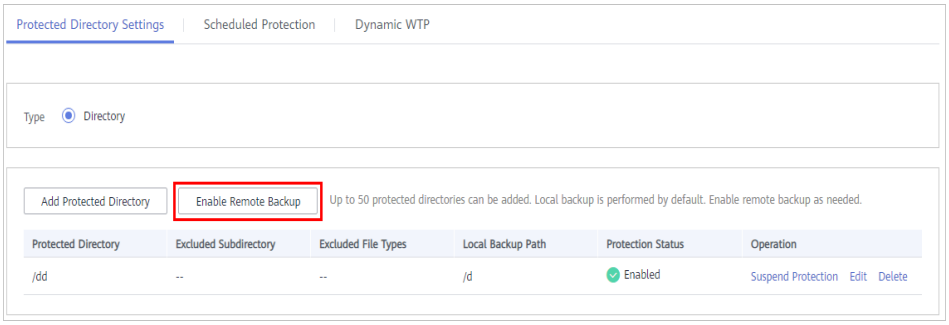
Step 6 Enable remote backup.

By default, HSS backs up the files from the protected directories (excluding specified subdirectories and file types) to the local backup directory you specified when adding protected directories. To protect the local backup files from tampering, you must enable the remote backup function.

For details about how to add a remote backup server, see **Adding a Remote Backup Server**.

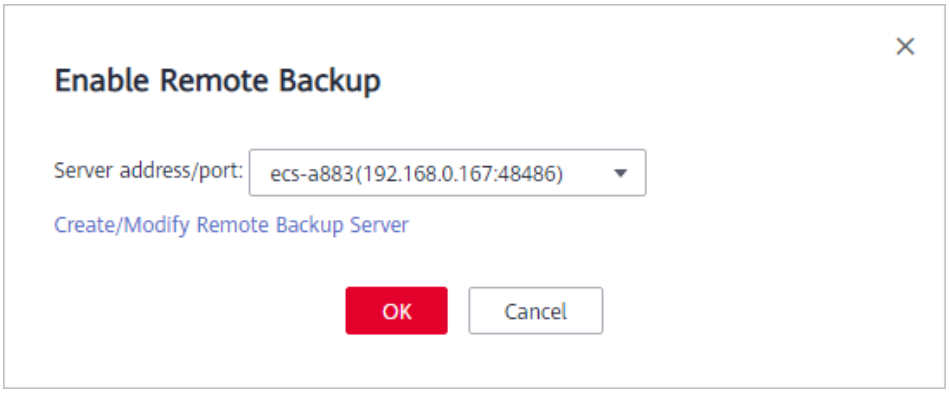
1. Click **Enable Remote Backup**.

Figure 10-3 Enabling remote backup



2. Select a backup server from the drop-down list box.

Figure 10-4 Setting remote backup



3. Click **OK**.

----End

Follow-Up Procedure

- Suspend protection: You can suspend WTP for a directory if needed. It is best practice that you resume WTP in a timely manner to prevent the files in the directory from being tampered with.
- Edit a protected directory: You can modify the added protected directory as needed.
- Delete a protected directory: You can delete the directories that do not need to be protected.

NOTICE

- After you suspend protection for a protected directory, delete it, or modify its path, files in the directory will no longer be protected. Before performing these operations, ensure you have taken other measures to protect the files.
- After you suspend protection for a protected directory, delete it, or modify its path, if you find your files missing in the directory, search for them in the local or remote backup path.

10.2 Adding a Remote Backup Server

By default, HSS backs up the files from the protected directories (excluding specified subdirectories and file types) to the local backup directory you specified when adding protected directories. To protect the local backup files from tampering, you must enable the remote backup function.

If a file directory or backup directory on the local server becomes invalid, you can use the remote backup service to restore the tampered web page.

Prerequisites

The following servers can be used as remote backup servers:

Huawei Cloud Linux servers whose **Server Status** is **Running** and **Agent Status** is **Online**

NOTICE

- The remote backup function can be used when the Linux backup server is connected to your cloud server. To ensure a proper backup, you are advised to select a backup server on the same intranet as your cloud server.
- You are advised to use intranet servers least exposed to attacks as the remote backup servers.

Configuring a Remote Backup Server

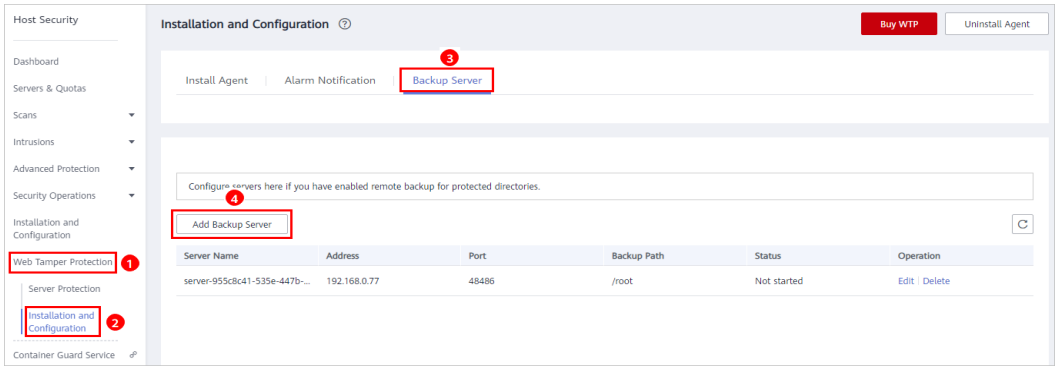
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Web Tamper Protection** > **Installation and Configuration**. Click the **Backup Server** tab and click **Add Backup Server**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-5 Configuring a backup server



Step 4 In the displayed dialog box, add a remote backup server and set required parameters. For details, see **Table 10-2**.

Figure 10-6 Adding a remote backup server

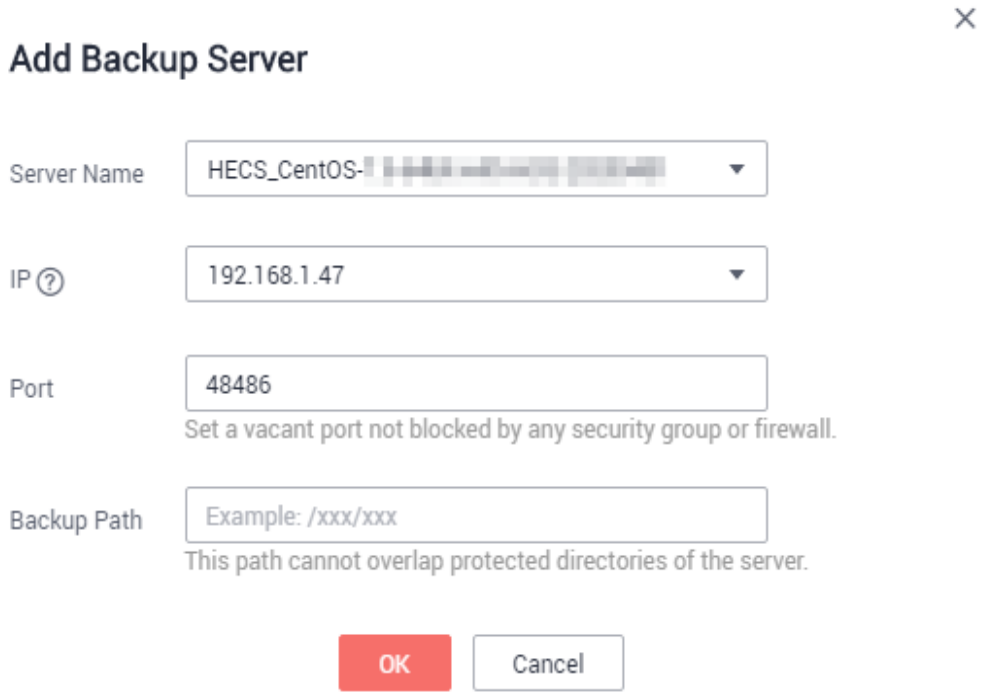


Table 10-2 Parameters for a remote backup server

Parameter	Description
Address	This address is the private network address of the Huawei Cloud server.
Port	Ensure that the port is not blocked by any security group or firewall or occupied.

Parameter	Description
Backup Path	Path of remote backup files. ● If the protected directories of multiple servers are backed up to the same remote backup server, the data will be stored in separate folders named after agent IDs. Assume the protected directories of the two servers are**/hss01** and **hss02**, and the agent IDs of the two servers are **f1fdbabc-6cdc-43af-acab-e4e6f086625f** and **f2ddbabc-6cdc-43af-abcd-e4e6f086626f**, and the remote backup path is **/hss01**. The corresponding backup paths are **/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f** and **/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f**. ● If WTP is enabled for the remote backup server, do not set the remote backup path to any directories protected by WTP. Otherwise, remote backup will fail.

Step 5 Click **OK**.

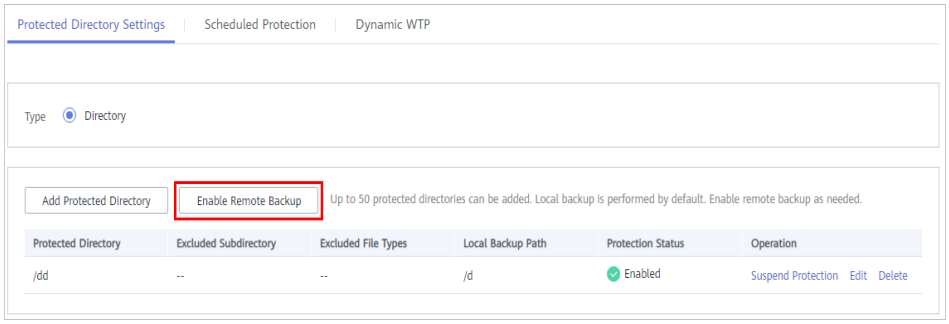
----End

Enabling Remote Backup

Step 1 Choose **Web Tamper Protection** > **Server Protection**. Click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

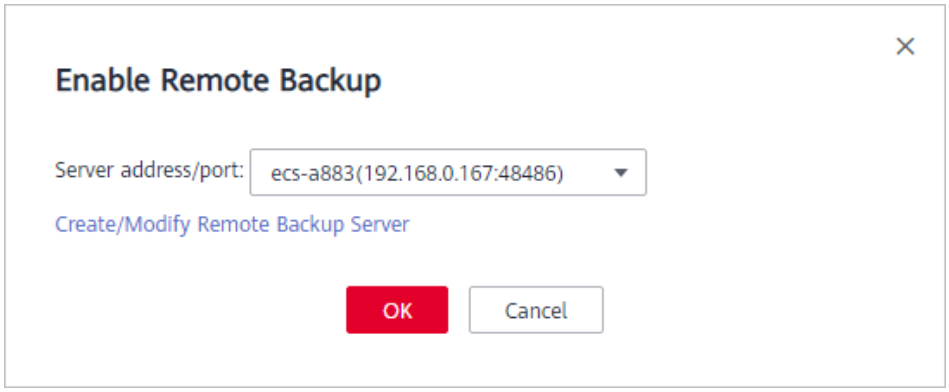
Step 2 Set **Type** to **Directory** and click **Enable Remote Backup**.

Figure 10-7 Enabling remote backup



Step 3 In the **Enable Remote Backup** drop-down list, select a server.

Figure 10-8 Setting remote backup



Step 4 Click **OK**.

----End

Follow-Up Procedure

Disabling remote backup

Exercise caution when performing this operation. If remote backup is disabled, HSS will no longer back up files in your protected directories.

10.3 Adding a Privileged Process That Can Modify Protected Files

After WTP is enabled, the content in the protected directories is read-only. To allow certain processes to modify files in the directories, you can add them to the privileged process list.

Only the modification made by privileged processes can take effect. Modifications made by other processes will be automatically rolled back.

Exercise caution when adding privileged processes. Do not let untrustworthy processes access your protected directories.

A maximum of 10 process file paths can be added to each server.

Prerequisites

- On the **Server Protection** page of the WTP console, the **Agent Status** of the target server is **Online**, and the **Protection Status** of the server is **Enabled**.
- You can configure privileged processes only for Windows OSs.

Adding a Privileged Process

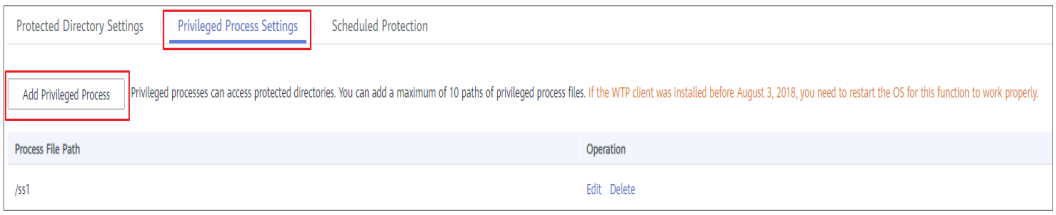
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Step 4 On the **Privileged Process Settings** tab, click **Add Privileged Process**.

Figure 10-9 Adding a privileged process



Step 5 In the **Add Privileged Process** dialog box, enter the path of the privileged process.

The process file path must contain the process name and extension, for example, **C:/Path/Software.type**. If the process has no extension, ensure the process name is unique.

Step 6 Click **OK**.

NOTE

If the HSS agent was installed before August 3, 2018, restart the OS after the privileged process is added.

----End

Follow-Up Procedure

Modifying or deleting existing privileged processes

In the **Operation** column of a process file path, click **Edit** to modify the privileged processes or click **Delete** to delete it if it is unnecessary.

NOTE

- After you edit or delete the process file path, the privileged process cannot modify the files in the protected directory. To avoid impact on services, exercise caution when performing these operations.
- Unnecessary processes may be exploited by attackers due to process vulnerabilities. Therefore, delete unnecessary privileged processes in a timely manner.

10.4 Setting Scheduled WTP Protection

You can schedule WTP protection to allow website updates in specific periods.

NOTE

Exercise caution when you set the periods to disable WTP, because files will not be protected in those periods.

Procedure

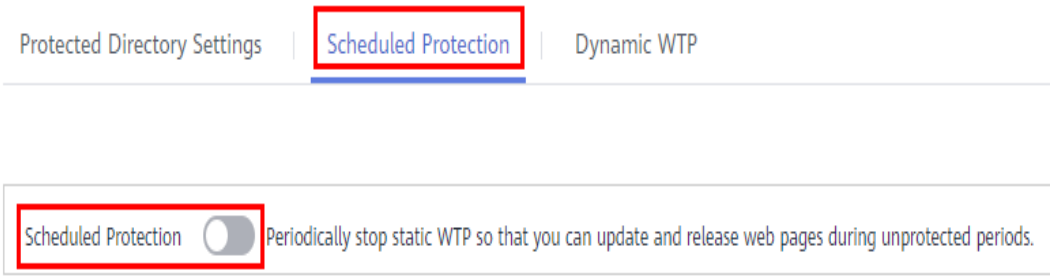
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Step 4 Enable scheduled protection.

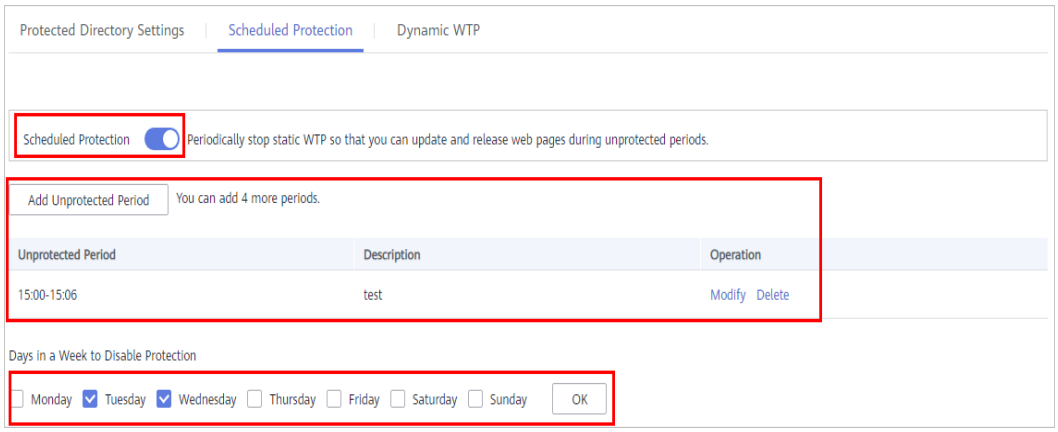
Figure 10-10 Scheduled protection



Step 5 Click **OK**.

Step 6 Set **Unprotected Period** and **Days in a Week to Disable Protection**.

Figure 10-11 Setting scheduled protection parameters



----End

Rules for Setting an Unprotected Period

- Unprotected period >= 5 minutes
- Unprotected period < 24 hours
- Periods (except for those starting at 00:00 or ending at 23:59) cannot overlap and must have an at least 5-minute interval.
- A period cannot span two days.
- The server time is used as a time base.

10.5 Enabling Dynamic WTP

Dynamic WTP protects your web pages while Tomcat applications are running, and can detect tampering of dynamic data, such as database data. It can be enabled with static WTP or separately.

Prerequisites

You are using a server running the Linux OS.

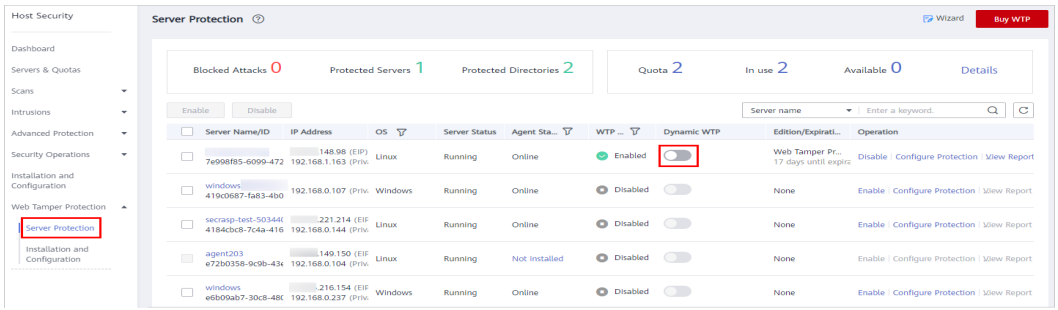
Procedure

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Web Tamper Protection** > **Server Protection**. Click in the **Dynamic WTP** column.

Figure 10-12 Enabling dynamic WTP



NOTE

Alternatively, click **Configure Protection** and click the **Dynamic WTP** tab. Click to enable dynamic WTP.

Step 4 In the **Enable Dynamic WTP** dialog box, click **OK**.

Step 5 Restart Tomcat for the function to take effect.

If you disable WTP and enable it again, you will have to restart Tomcat for the setting to take effect.

----End

10.6 Viewing WTP Reports

Once WTP is enabled, the HSS service will comprehensively check protected directories you specified. You can check records about detected tampering attacks.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

Agent Status of the server is **Online**, and its **WTP Status** is **Enabled**.

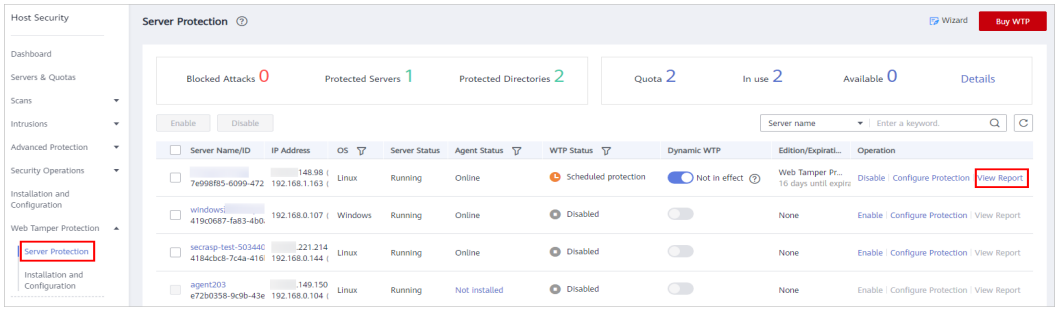
Procedure

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the WTP console, Choose **Server Protection**. Click **View Report** in the **Operation** column.

Figure 10-13 Viewing a protection record



Step 4 View details on the report page.

Figure 10-14 Static WTP records

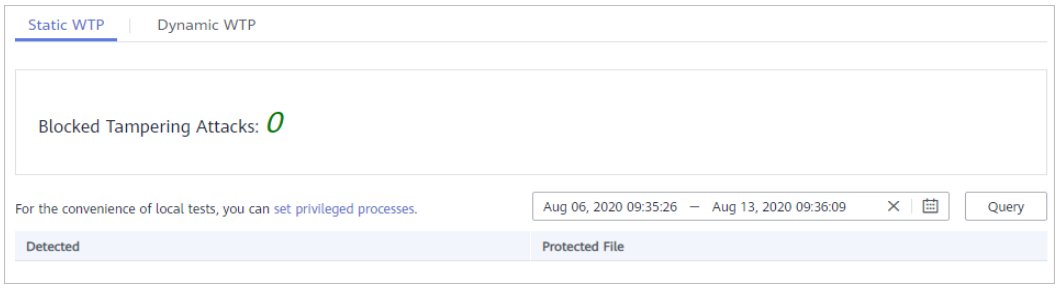
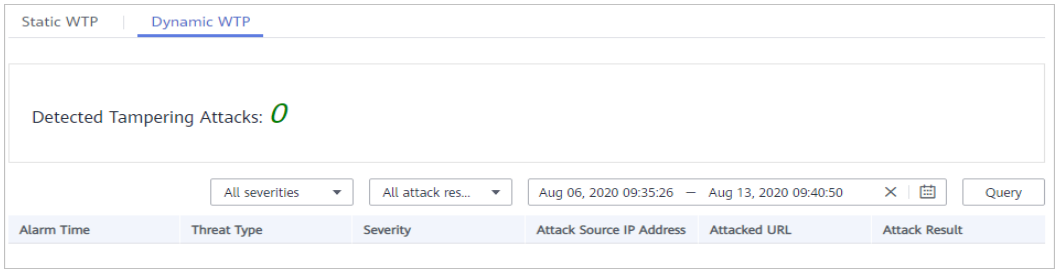


Figure 10-15 Dynamic WTP records



----End

11 Managing Quotas

11.1 Viewing Quotas

You can check, renew, and unsubscribe from your quota in the server list.

Only the quota purchased in the selected region is displayed. If your quota is not found, ensure you have switched to the correct region and search again.

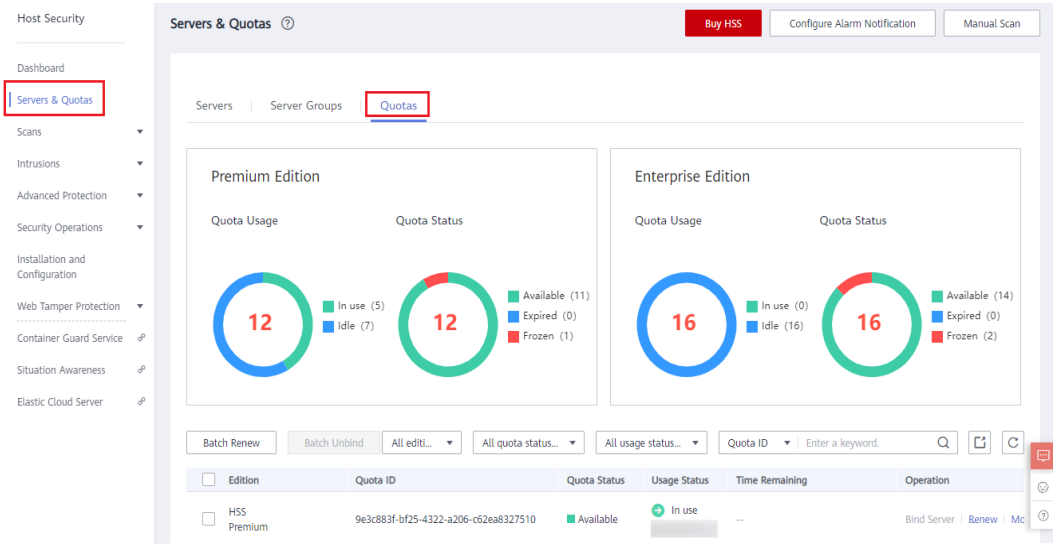
Viewing Enterprise/Premium Quota

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Servers** page, click the **Quotas** tab.

Figure 11-1 Viewing the HSS quota



Step 4 Check quotas and the servers bound to them.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-1 Parameters

Parameter	Description
Edition	Quota edition
Quota ID	Quota ID
Quota Status	• **Available**: The quota has not expired and can be used properly. • **Expired**: The quota has expired. During this period, you can still use the quota. • **Frozen**: The quota no longer protects your servers. When the frozen period expires, the quota will be permanently deleted.
Usage Status	• **In use**: The quota is being used for a server. The name of the server is displayed below the status. • **Idle**: The quota is not in use.

NOTE

- Binding quota to a server

  Choose **Servers**, click the **Quotas** tab, and click **Bind Server** in the **Operation** column.

  A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- Renewal

  You can click **Renew** in the **Operation** column of the quota to renew it. For details, see **How Do I Renew HSS?**.
- Unsubscription

  You can click **Unsubscribe** in the **Operation** column of the quota to unsubscribe from it. For details, see **How Do I Apply for Unsubscription and Refund?**.
- Unbinding quota

  On the **Quotas** tab of the **Servers** page, choose **More** > **Unbind Quota** in the **Operation** column of a quota. HSS will automatically disable protection for the corresponding server and the quota status will change to **Idle**.

----End

Viewing WTP Quota

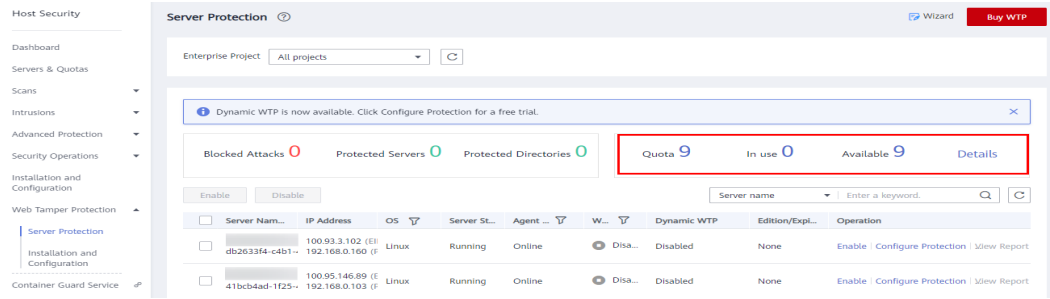
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Web Tamper Protection**.

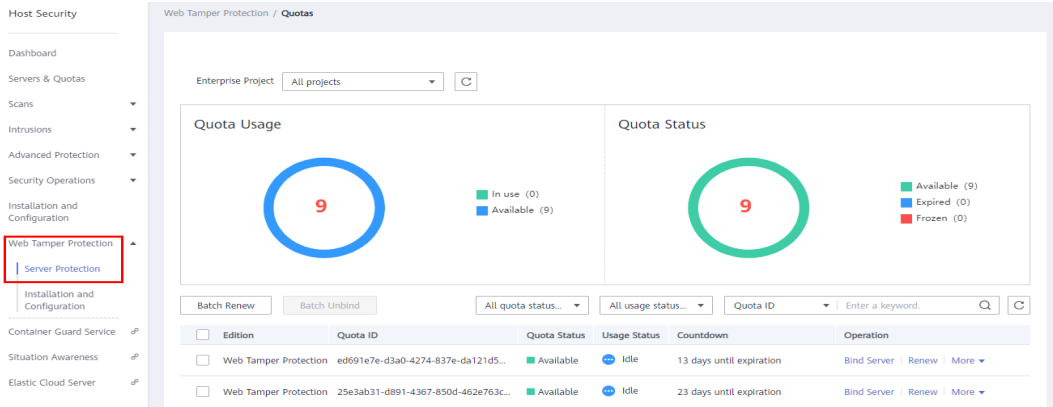
 Copyright © Huawei Technologies Co., Ltd.

Figure 11-2 Viewing the WTP edition HSS quota



Step 4 Click **Details**.

Figure 11-3 Quota details



Step 5 Check quota details.

Table 11-2 Parameters

Parameter	Description
Quota Status	• **Available**: The quota has not expired and can be used properly. • **Expired**: The quota has expired. During this period, you can still use the quota. • **Frozen**: The quota no longer protects your servers. When the frozen period expires, the quota will be permanently deleted.
Usage Status	• **In use**: The quota is being used for a server. The name of the server is displayed below the status. • **Idle**: The quota is not in use.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- Binding quota to a server

  To enable WTP protection for a server, you can also choose **Web Tamper Protection** > **Server Protection**, click **Details**, and click **Bind Server** in the **Operation** column of a quota.

  A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- Renewal

  You can click **Renew** in the **Operation** column of the edition to renew the subscription to WTP edition HSS. For details, see **How Do I Renew HSS?**.
- Unsubscription

  You can click **Unsubscribe** in the **Operation** column of the edition to unsubscribe from the subscription to WTP edition HSS. For details, see **How Do I Apply for Unsubscription and Refund?**.
- Unbind Quota

  Choose **Web Tamper Protection** > **Server Protection**, click **Details**, and choose **More** > **Unbind Quota** in the **Operation** column of a quota. HSS will automatically disable WTP for the corresponding server and the quota status will change to **Idle**.

----End

11.2 Binding a Quota to a Server

A quota can be bound to a server to protect it, on condition that the agent on the server is online.

Prerequisites

- The agent has been installed on the server you want to protect.
- The quota is in **Available** state and its **Usage Status** is **Idle**.

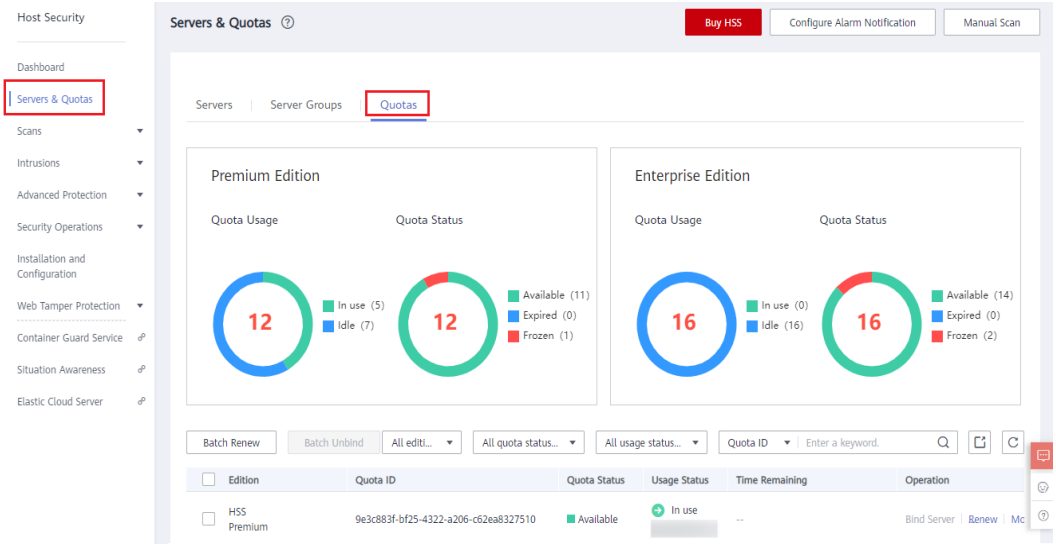
Procedure

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Servers** page, click the **Quotas** tab.

Figure 11-4 Viewing the HSS quota

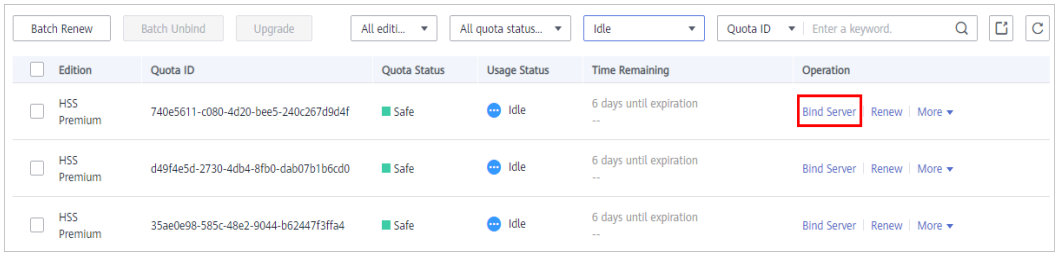


Step 4 On the quota details page, click **Bind Server** in the row of the quota.

NOTE

To enable WTP protection for a server, you can also choose **Web Tamper Protection** > **Server Protection**, click **Details**, and click **Bind Server** in the **Operation** column of a quota.

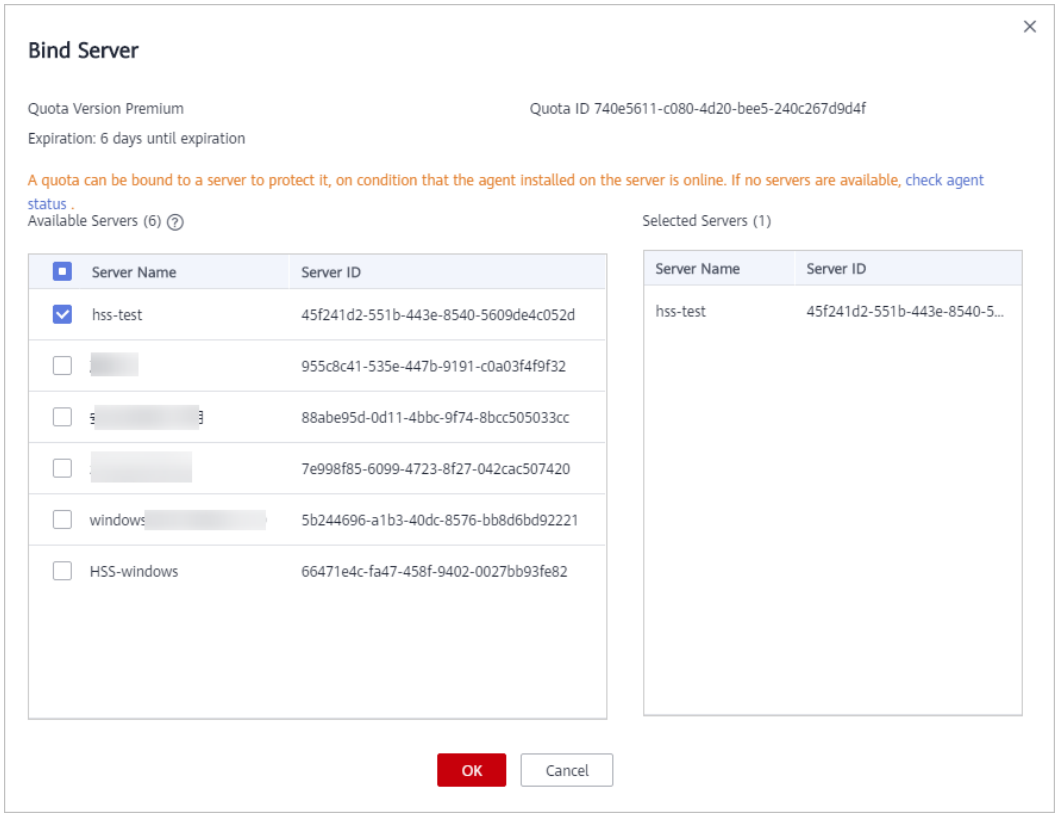
Figure 11-5 Binding quota to a server



Step 5 Select a server.

 Copyright © Huawei Technologies Co., Ltd.

Figure 11-6 Selecting a server to be bound



Step 6 Click **OK**. HSS will automatically enable protection for the server.

----End

11.3 Upgrading a Quota

You can upgrade your HSS quota to the enterprise or premium edition as needed.

To use the WTP edition, purchase it separately. For details, see .

Prerequisites

- You have purchased the basic or enterprise edition HSS.
- The quota is in **Normal** state and its **Usage Status** is **Idle**.
- The quotas to be upgraded are in the same edition.

Upgrading Quotas

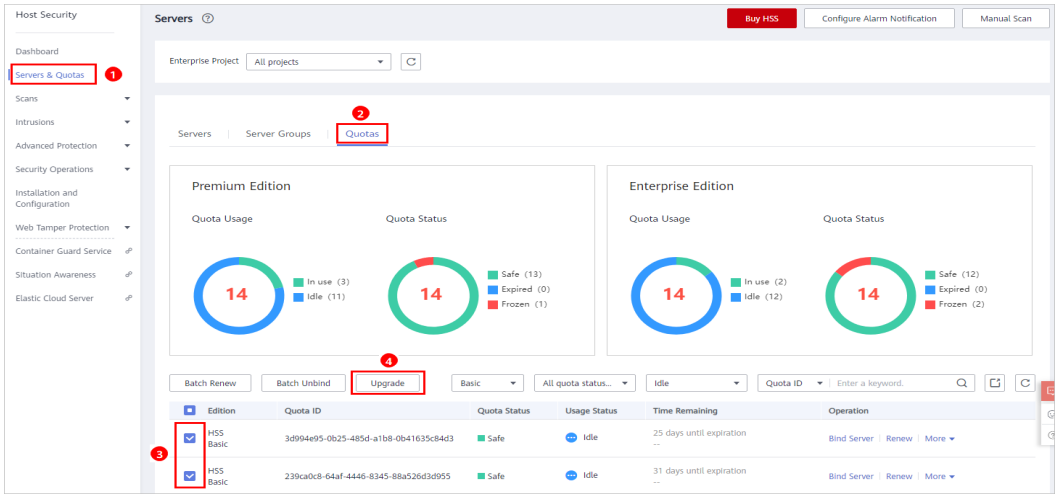
Step 1 **Log in to the management console.**

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Servers**. Click the **Quotas** tab. Select quotas and click Upgrade, as shown in **Figure 11-7**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 11-7 Upgrading quotas



Step 4 On the **Upgrade HSS** page, select and confirm the target edition.

1. Select the target edition.

   Select **Enterprise** or **Premium**. For details about the differences between editions, see **Editions**.

   Your target edition options vary according to your current quota editions.

   – If you are using the basic edition,

     Select **Enterprise** or **Premium**.

   – If you are using the enterprise edition,

     Select **Premium**.

2. Confirm quota details.

   – Confirm the **Current Region**, **Billing Mode**, **Current Edition**, and **Target Edition** of your quotas.

   – Fix reported issues (if any).

     ▪ Quotas in **Frozen** or **Expired** state cannot be upgraded.

       You can remove or renew them.

     ▪ Quotas in **In Use** state cannot be upgraded.

       You can suspend protection during upgrade or remove the quotas.

       NOTE

       If you choose to suspend protection during upgrade, servers protected by the upgraded quotas may be interrupted. Exercise caution when performing this operation.

Step 5 In the lower right corner of the page, click **Next**.

For details about pricing, see **Product Pricing Details**.

Step 6 After confirming that the order, select **I have read and agree to the Host Security Service Disclaimer** and click **Pay Now**.

Step 7 Click **Pay** and complete the payment.

----End

 Copyright © Huawei Technologies Co., Ltd.

11.4 Unbinding a Quota from a Server

You can unbind quotas from servers that no longer need to be protected. Exercise caution when performing this operation, because unprotected servers are exposed to security risks.

After unbinding a quota, you can bind it to another server or unsubscribe from it to reduce cost.

Mechanism

- You can manually unbind a cloud server from the HSS quota on the **Servers** page.
- The server will be automatically unbound from the HSS quota 30 days after the Agent goes offline.

Prerequisites

The quotas to be unbound are in use.

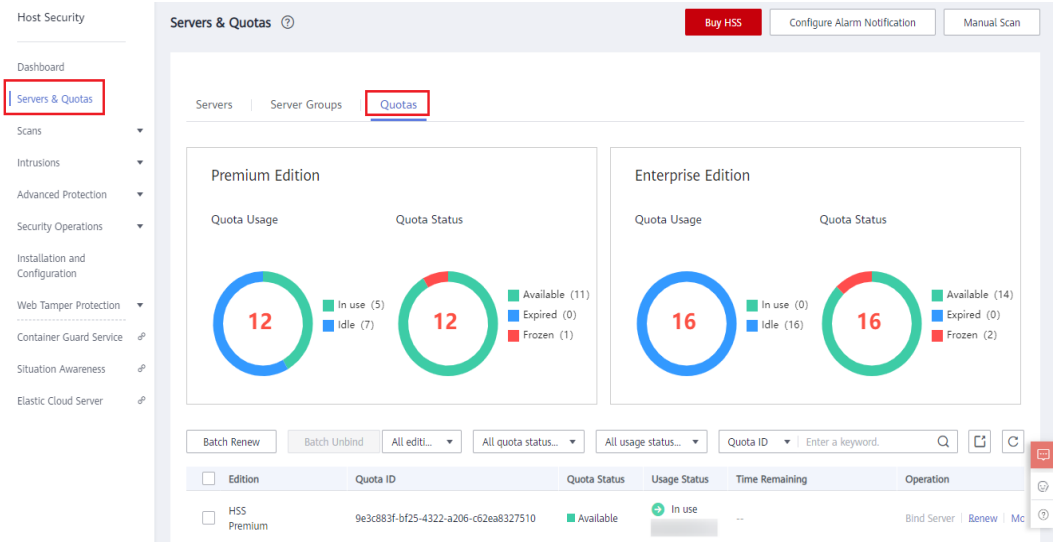
Unbinding Basic/Enterprise/Premium Edition Quota

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 On the **Servers** page, click the **Quotas** tab.

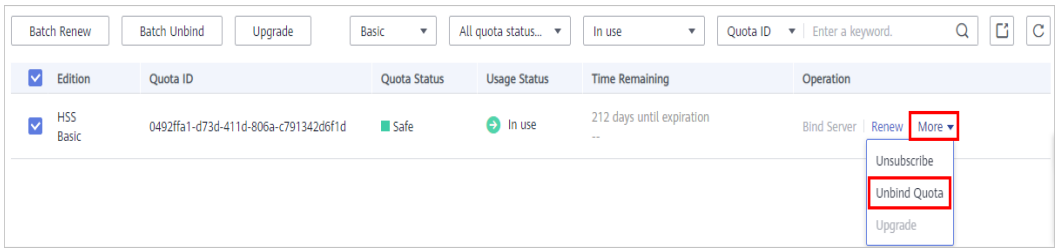
Figure 11-8 Viewing the HSS quota



Step 4 In the quota list, choose **More** > **Unbind Quota**, as shown in **Figure 11-9**.

Copyright © Huawei Technologies Co., Ltd.

Figure 11-9 Unbinding quota



NOTE

To unbind multiple quotas at a time, select them and click **Batch Unbind**. Exercise caution when performing this operation, because unprotected servers are exposed to security risks.

Step 5 In the displayed dialog box, click **OK** to unbind the quota.

----End

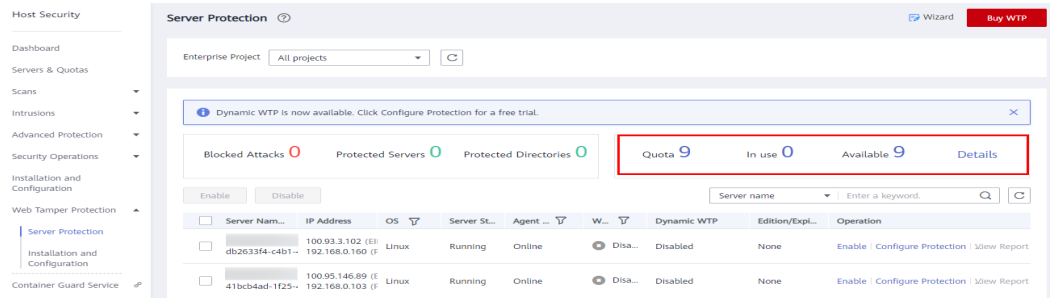
Unbinding WTP Quota

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

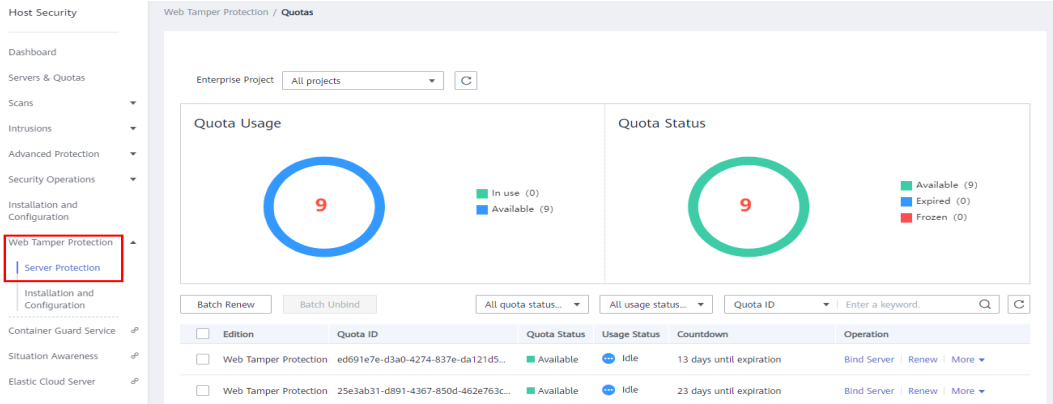
Step 3 In the navigation pane, choose **Web Tamper Protection**.

Figure 11-10 Viewing the WTP edition HSS quota



Step 4 Click **Details**.

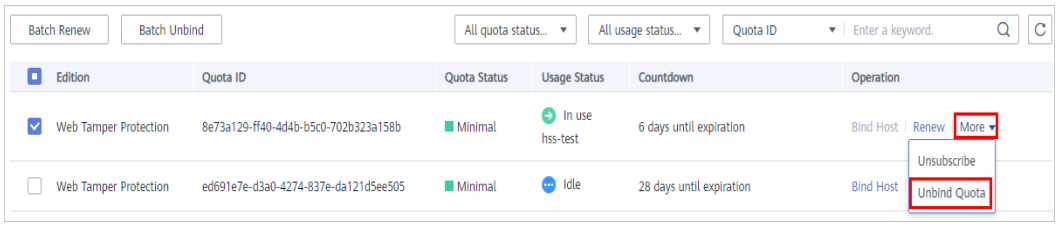
Figure 11-11 Quota details



Copyright © Huawei Technologies Co., Ltd.

Step 5 In the quota list, choose **More** > **Unbind Quota**, as shown in **Figure 11-12**.

Figure 11-12 Unbinding WTP quota



NOTE

To unbind multiple quotas at a time, select them and click **Batch Unbind**. Exercise caution when performing this operation, because unprotected servers are exposed to security risks.

Step 6 In the confirmation dialog box, click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

12 (Optional) Managing Enterprise Projects

12.1 Managing Projects and Enterprise Projects

Selections are available only if you have enabled the enterprise project function, or your account is an enterprise account. To enable this function, contact your customer manager. An enterprise project provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.

Creating a Project and Assigning Permissions

- Creating a project

  Log in to the management console, click the username in the upper right corner, and select **Identity and Access Management**. In the navigation pane on the left, choose **Projects**. In the right pane, click **Create Project**. On the displayed **Create Project** page, select a region and enter a project name.

- Granting permissions

  You can assign permissions (of resources and operations) to user groups to associate projects with user groups. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. On the **User Groups** page, locate the target user group and click **Configure Permission** in the **Operation** column. The **User Group Permissions** page is displayed. Locate the row that contains the target project, click **Configure Policy**, and select the required policies for the project.

  b. On the **Users** page, locate the target user and click **Modify** in the **Operation** column. In the **User Groups** area, add a user group for the user.

Creating an Enterprise Project and Assigning Permissions

- Creating an enterprise project

  On the management console, click **Enterprise** in the upper right corner. The **Enterprise Management** page is displayed. In the navigation pane on the

left, choose **Enterprise Project Management**. In the right pane, click **Create Enterprise Project** and enter a name.

NOTE

Enterprise is available on the management console only if you have enabled the enterprise project, or you have an enterprise account. To enable this function, contact customer service.

- Granting permissions

  You can add a user group to an enterprise project and configure a policy to associate the enterprise project with the user group. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. Locate the row that contains the target enterprise project, click **More** in the **Operation** column, and select **View User Group**. On the displayed **User Groups** page, click **Add User Group**. In the displayed **Add User Group** dialog box, select the user groups you want to add and move them to the right pane. Click **Next** and select the policies.

  b. In the navigation pane on the left, choose **Personnel Management** > **User Management**. Locate the row that contains the target user, click **More** in the **Operation** column, and select **Add to User Group**. In the displayed **Add to User Group** dialog box, select the user groups for which policies have been configured and click **OK**.

- Associating HSS with enterprise projects

  You can use enterprise projects to manage cloud resources.

  – Select an enterprise project when purchasing HSS.

    On the page for buying HSS, select an enterprise project from the **Enterprise Project** drop-down list.

  – Adding resources

    On the **Enterprise Project Management** page, you can add existing ECSs/BMSs to an enterprise project.

    Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.

  For more information, see**Creating an Enterprise Project**.

12.2 Managing All Projects Settings

If you have enabled the enterprise project function, you can select **All projects** from the **Enterprise Project** drop-down list and batch set all servers under all your projects.

- Binding quotas to servers

  Under **All projects**, you can bind the quota of an enterprise project to a server of another project. The project that the quota belongs to will be billed for the quota.

- Batch installation and configuration

  Configure the alarm whitelist, login whitelist, malicious program isolation and killing, and alarm notifications for all servers.

- Applying a policy group

  The policy groups under **All projects** can be applied to any servers in any enterprise projects protected by the premium edition.

  The policy groups under **All projects** do not belong to any specific projects and do not affect the policy groups under any other projects.

- Subscribing to security reports under **All projects**

  The security reports under **All projects** do not belong to any specific projects and do not affect the security reports under any other projects.

You can configure uniform settings for all projects under **All projects** and customize settings under a specific project. The settings under an enterprise project do not affect those under other enterprise projects.

Prerequisites

You have the **Tenant Administrator** or **HSS Administrator+Tenant Guest** permissions.

Binding Quotas to Servers

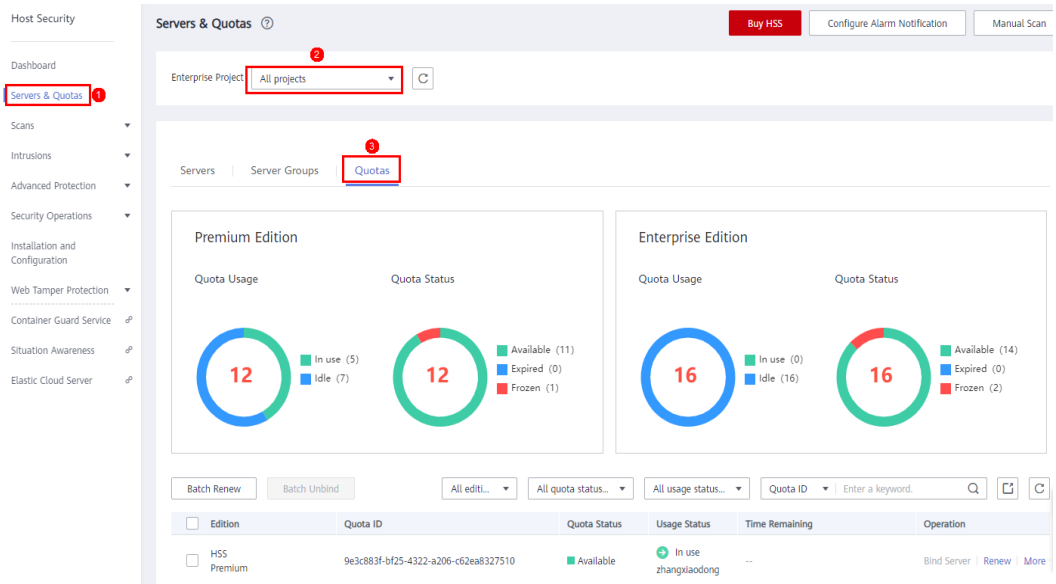
Perform the following steps to bind a premium edition quota to a server under **All projects**.

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Servers** and select **All projects** from the **Enterprise Project** drop-down list. Click the **Quotas** tab.

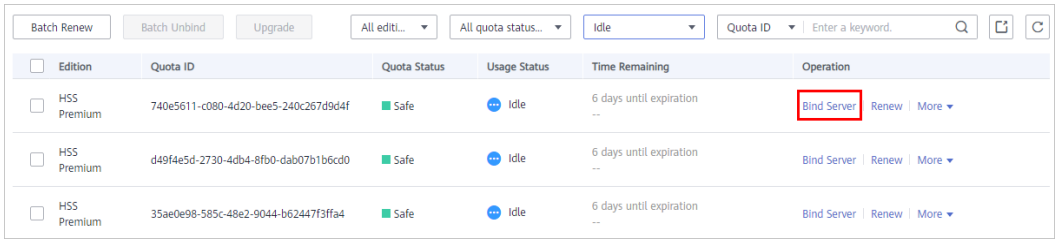
Figure 12-1 Protection quotas



Step 4 In the quota list, select a quota whose **Usage Status** is **Idle** and click **Bind Server**.

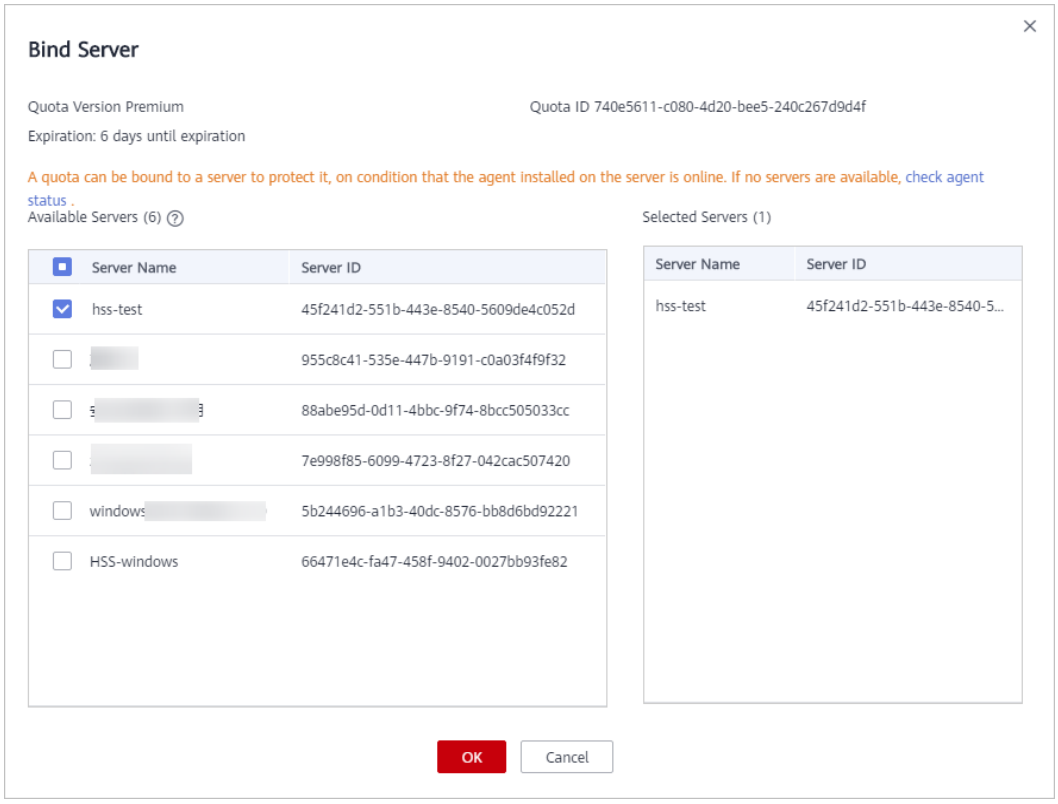
Copyright © Huawei Technologies Co., Ltd.

Figure 12-2 Binding a quota to a server



Step 5 Select servers in the **Details** dialog box.

Figure 12-3 Binding a quota



Step 6 Click **OK**. The **Protection Status** of the server will change to **Enabled**.

----End

Batch Installation and Configuration

You can configure settings under **All projects** and apply them to all projects at a time. However, this does not mean the settings of all your projects have to be the same. You can customize settings for specific projects.

NOTICE

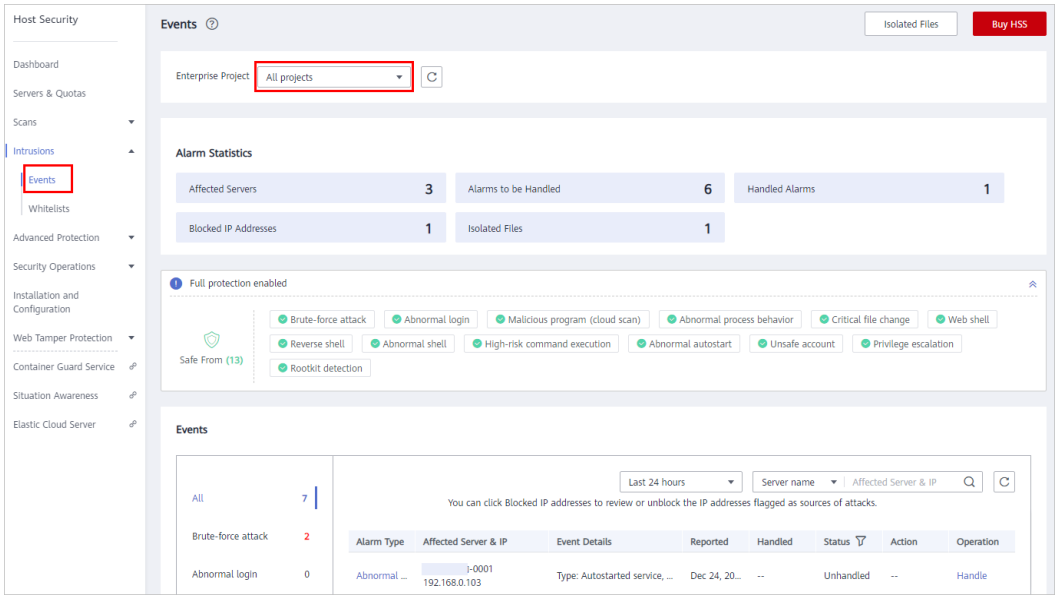
Under **All projects**, you can configure the following items in batches: alarm whitelist, login whitelist, automatic isolation and killing of malicious programs, and alarm notifications.

 Copyright © Huawei Technologies Co., Ltd.

Perform the following steps to configure the alarm whitelist under **All projects** and apply them to **Project 1** and **Project 2**:

Step 1 Choose **Intrusions** > **Events**.

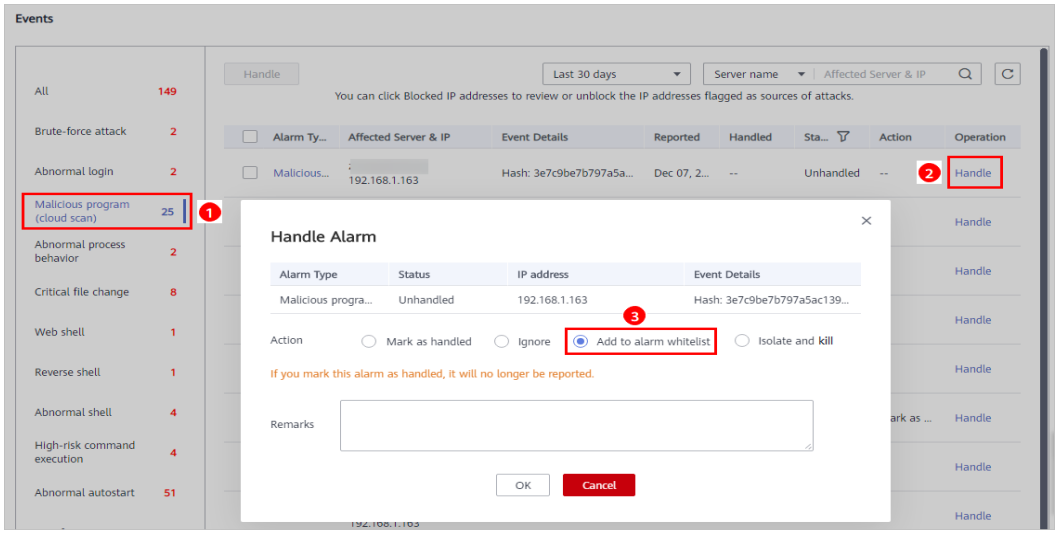
Figure 12-4 Event list



Step 2 Select **All Projects** from the **Enterprise Project** drop-down list.

Step 3 In the event list, whitelist an alarm, for example, an alarm of the **Malicious program (cloud scan)** type.

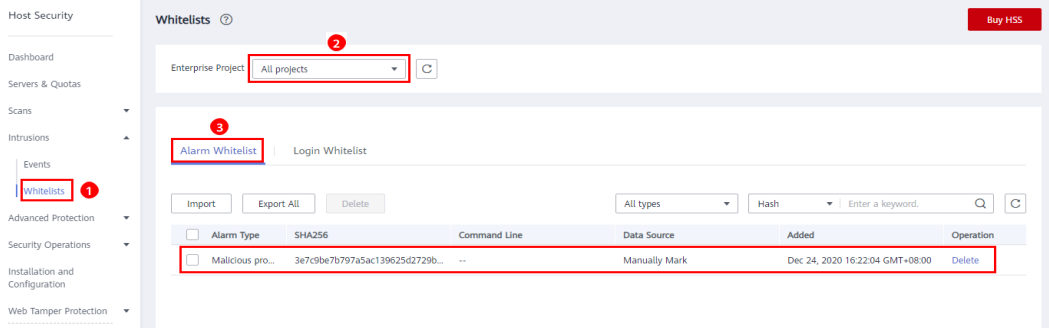
Figure 12-5 Adding an alarm to the alarm whitelist



Step 4 Choose **Intrusions** > **Whitelists**. Select **All projects** from the **Enterprise Project** drop-down list. Click the **Alarm Whitelist** tab.

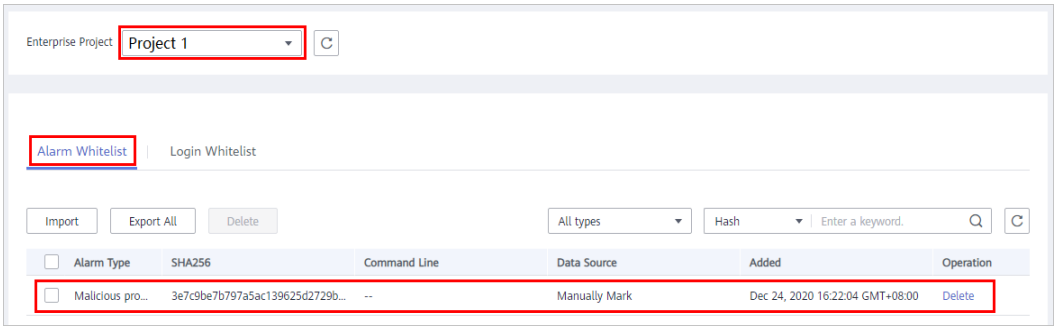
Copyright © Huawei Technologies Co., Ltd.

Figure 12-6 Alarm whitelist



Step 5 Switch projects in the **Enterprise Project** drop-down list, to check the settings of **Project 1** and **Project 2**, respectively. Confirm that **Malicious program (cloud scan)** has been added to the alarm whitelist of both projects.

Figure 12-7 Alarm whitelist of Project 1



Step 6 (Optional) To enable alarms on **Malicious program (cloud scan)**, remove it from the alarm whitelist of **Project 2**.

The modification in **Project 2** does not affect **Project 1**.

----End

Applying a Policy Group

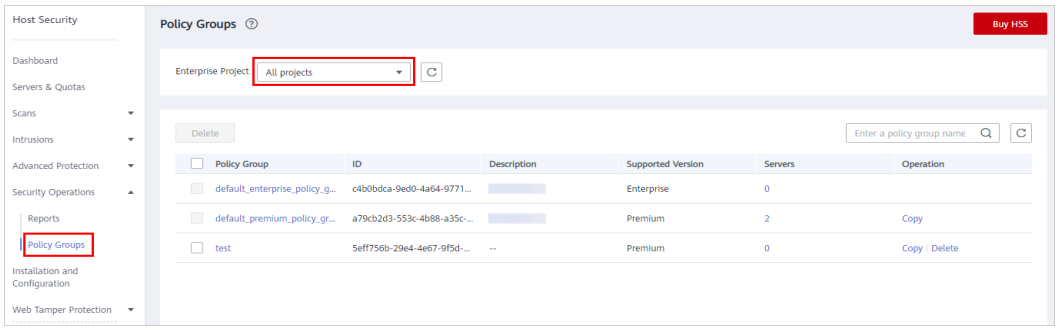
The policy groups under **All projects** can be applied to any servers in any enterprise projects protected by the premium edition.

Perform the following steps to create a policy group named **hss_test** under **All Projects** and apply the policy group to any server protected by the premium edition.

Step 1 Choose **Security Operations** > **Policies** and switch to **All projects**. Click **Copy** next to a group.

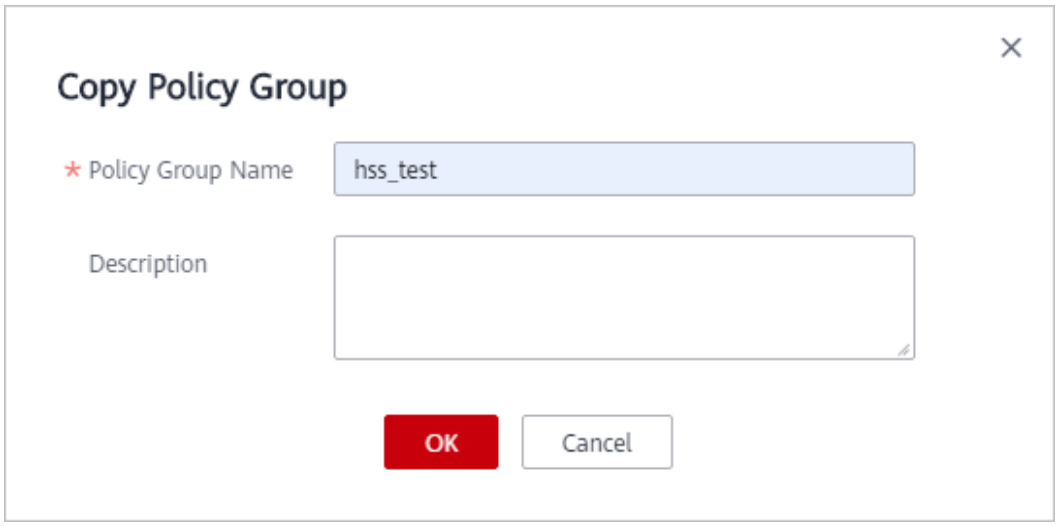
 Copyright © Huawei Technologies Co., Ltd.

Figure 12-8 Copying the default policy group



Step 2 In the dialog box that is displayed, enter a policy group name, for example, **hss_test**.

Figure 12-9 Configuring a policy group

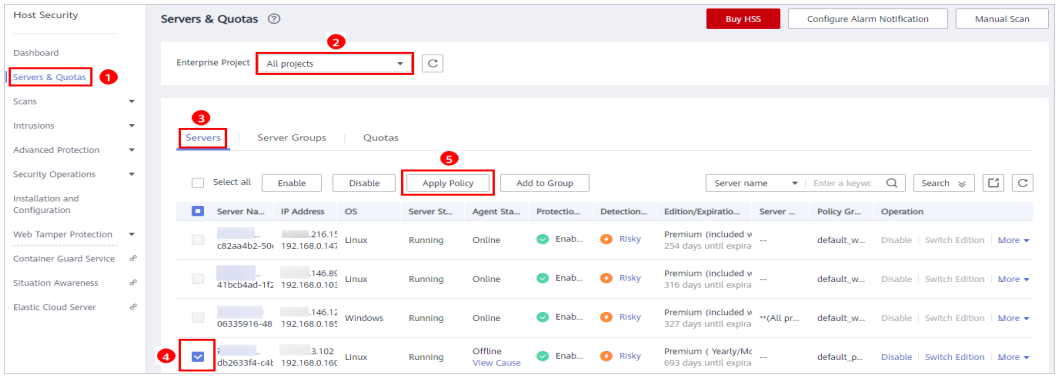


Step 3 Click **OK**.

You can click a group name to modify its settings.

Step 4 Choose **Servers** and switch to **All projects**. Select a server protected by the premium edition, click **Apply Policy**, and deploy the **hss_test** policy group.

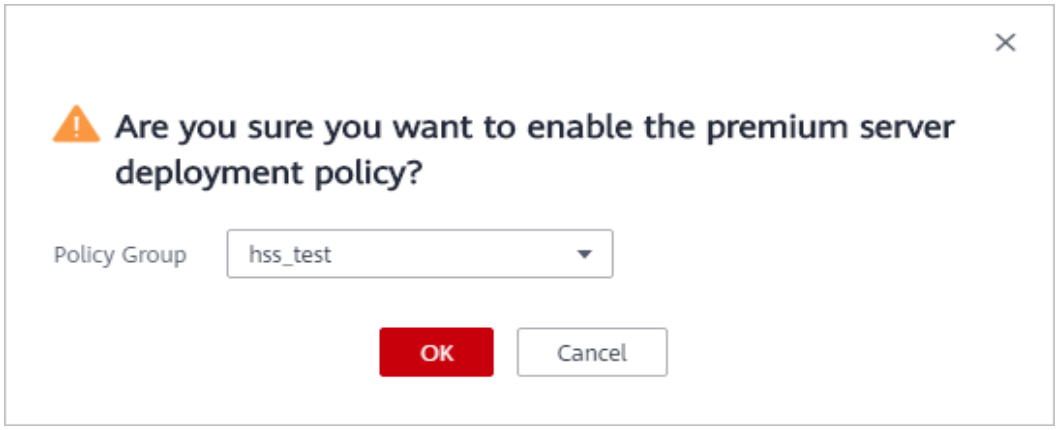
Figure 12-10 Applying a policy



Step 5 In the dialog box that is displayed, select the policy group you created, as shown in **Figure 12-11**.

Copyright © Huawei Technologies Co., Ltd.

Figure 12-11 Selecting a policy group



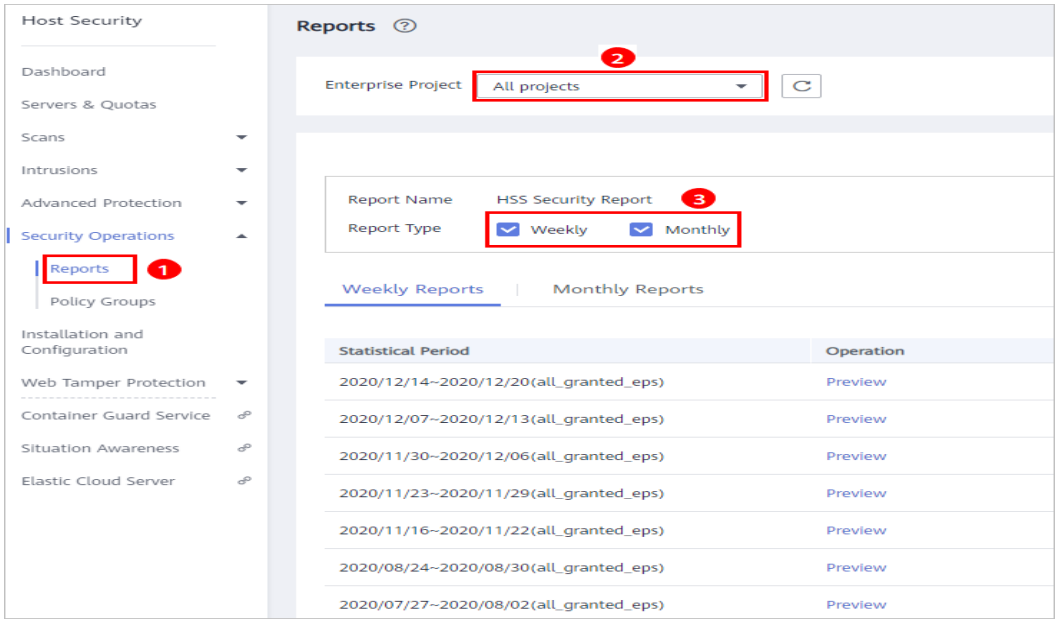
Step 6 Click **OK**.

----End

Subscribing to Security Reports Under All projects

Choose **Security Operations** > **Reports**, switch to **All projects**, and select **Weekly** and **Monthly**.

Figure 12-12 Subscribing to security reports under **All projects**



 Copyright © Huawei Technologies Co., Ltd.

13 Audit

13.1 HSS Operations Supported by CTS

Cloud Trace Service (CTS) records all operations on HSS, including requests initiated from the management console or open APIs and responses to the requests, for tenants to query, audit, and trace.

Table 13-1 lists HSS operations recorded by CTS.

Table 13-1 HSS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Enabling HSS	hss	openHssProtect
Disabling HSS	hss	closeHssProtect
Starting a manual detection	hss	manualDetection
Unblocking an IP address	hss	unblockIp
Configuring common login locations	hss	setCommonLocation
Configuring a login IP address whitelist	hss	setWhiteIpList
Enabling or disabling a login IP address whitelist	hss	switchWhiteIpList
Ignoring a port	hss	ignorePort
Unignoring a port	hss	noIgnorePort
Ignoring a risky configuration	hss	ignoreConfigRisky
Unignoring a risky configuration	hss	notIgnoreConfigRisky
One-click vulnerability fix	hss	repairVul

 Copyright © Huawei Technologies Co., Ltd.

Operation	Resource Type	Trace Name
Verifying a vulnerability	hss	verifyVul
Waiting for system restart and verification after one-click fix	hss	confirmVul
Ignoring a software vulnerability	hss	ignoreVul
Unignoring a software vulnerability	hss	notIgnoreVul
Enabling a firewall	HSS	turnonFirewall
Enabling WTP	HSS	openWtp
Disabling WTP	hss	stopWtp
Adding a protected directory to WTP	hss	addWtpDir
Removing a protected directory from WTP	hss	deleteWtpDir
Changing a protected directory in WTP	hss	modifyWtpDir
Suspending protection for a protected directory in WTP	hss	suspendWtpDir
Resuming protection for a protected directory in WTP	hss	resumeWtpDir
Setting a backup server for WTP	hss	setWtpBackupHost
Setting remote backup for WTP	hss	setWtpRemoteBackup
Adding a privileged process in WTP	hss	addWtpPrivilegedProcess
Removing a privileged process from WTP	hss	deleteWtpPrivilegedProcess
Modifying a privileged process in WTP	hss	modifyWtpPrivilegedProcess
Enabling two-factor authentication	hss	turnOnTwoFactor
Disabling two-factor authentication	hss	turnOffTwoFactor
Changing the topic for two-factor authentication	hss	modifyTwoFactorTopic
Ignoring web shells	hss	ignoreWebShell
Unignoring web shells	hss	notIgnoreWebShell

 Copyright © Huawei Technologies Co., Ltd.

Operation	Resource Type	Trace Name
Uninstalling the agent	hss	unInstall
Setting a protection mode in WTP	hss	setProtectMode
Adding a protected file system in WTP	hss	addFileSystem
Removing a protected file system from WTP	hss	delFileSystem
Modifying a protected file system in WTP	hss	modifyFileSystem
Suspending protection for a file system in WTP	hss	suspendFileSystem
Resuming protection for a file system in WTP	hss	resumeFileSystem
Enabling unprotected periods in WTP	hss	turnonTimedStopProtect
Disabling unprotected periods in WTP	hss	turnoffTimedStopProtect
Setting unprotected periods in WTP	hss	setTimedStopDate
Adding unprotected periods in WTP	hss	addTimerRange
Modifying unprotected periods in WTP	hss	modifyTimerRange
Deleting unprotected periods from WTP	hss	delTimerRange
Setting WTP alarms	hss	setWtpAlertConfig
Enabling dynamic WTP	hss	turnonRasp
Disabling dynamic WTP	hss	turnoffRasp
Subscribing to reports	hss	subSafetyReport
Automatically isolating and killing malicious programs	hss	turnOnMPAutomatic
Stop isolating and killing malicious programs	hss	turnOffMPAutomatic
Importing the alarm whitelist	hss	importAlarmWhitelist
Removing alarms from whitelist	hss	deleteAlarmWhitelist
Exporting the alarm whitelist	hss	exportAlarmWhitelist

 Copyright © Huawei Technologies Co., Ltd.

Operation	Resource Type	Trace Name
Managing the login whitelist	hss	operateLoginWhitelist
Managing events	hss	operateEventStatus
Cancel file isolation	hss	deleteProcessIsolation-Rule
Modifying a policy group	hss	modifyPolicyGroup
Removing a policy group	hss	deletePolicyGroup
Copying a policy group	hss	copyPolicyGroup
Modifying a policy group	hss	modifyPolicyContent
Applying a policy	hss	deployPolicyGroup
Adding a server group	hss	addHostGroup
Deleting a server group	hss	deleteHostGroup
Modifying a server group	hss	modifyHostGroup
Adding a server to a group	hss	insertHostGroup
Enabling or disabling file integrity management	hss	switchKeyfiles
Manage application recognition events	hss	operateAppWhiteListE-vent
Creating a whitelist policy	hss	replaceAppWhiteListPoli-cy
Enabling or disabling a whitelist policy	hss	switchAppWhiteListPolicy
Deleting a whitelist policy	hss	deleteAppWhiteListPolicy
Managing whitelisted applications	hss	operateAppWhiteListPo-licyApp
Removing a server associated with a policy	hss	deleteAppWhiteListHos-tInfo
Associating servers	hss	addAppWhiteListHostIn-fo
Managing ransomware events	hss	operateAppRansomEven-tInfo
Creating or editing a ransomware prevention policy	hss	replaceAppRansomPoli-cyInfo
Deleting a ransomware prevention policy	hss	deleteAppRansomPoli-cyInfo

 Copyright © Huawei Technologies Co., Ltd.

Operation	Resource Type	Trace Name
Marking the ransomware status of a process	hss	operateAppRansomHashInfo
Removing a server associated with a ransomware prevention policy	hss	deleteAppRansomHostInfo
Associating a server with a ransomware prevention policy	hss	addAppRansomHostInfo
Relearning a ransomware prevention policy on associated servers	hss	relearnAppRansomHostInfo

13.2 Viewing Audit Logs

After you enable CTS, the system starts recording operations on HSS. Operation records for the last seven days can be viewed on the CTS console.

Viewing an HSS Trace on the CTS Console

Step 1 Log in to the management console.

Step 2 Click ☰ on the top of the page and choose **Cloud Trace Service** under **Management & Governance**. The CTS console is displayed.

Step 3 Choose **Trace List** in the navigation pane.

Step 4 Click **Filter** and specify filtering criteria as needed. The following four filters are available:

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**.

  Select the filter from the drop-down list.

  – Set **Trace Type** to **Management**.

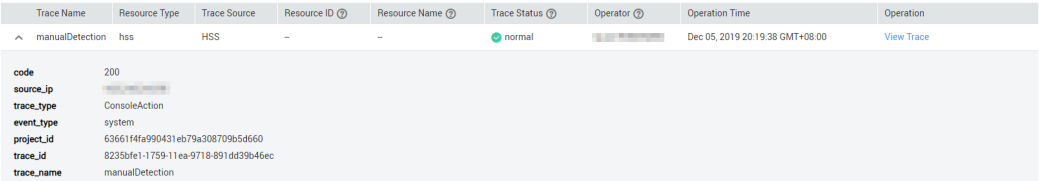
  – Set **Trace Source** to **HSS**.

  – When you select **Trace name** for **Search By**, you also need to select a specific trace name. When you select **Resource ID** for **Search By**, you also need to select or enter a specific resource ID. When you select **Resource name** for **Search By**, you also need to select or enter a specific resource name.
- **Operator**: Select a specific operator (a user other than tenant).
- **Trace Rating**: Available options include **All trace status**, **normal**, **warning**, and **incident**. You can only select one of them.
- **Time Range**: In the upper right corner of the page, you can query traces in the last 1 hour, last 1 day, last 1 week, or within a customized period.

Step 5 Click **Query**.

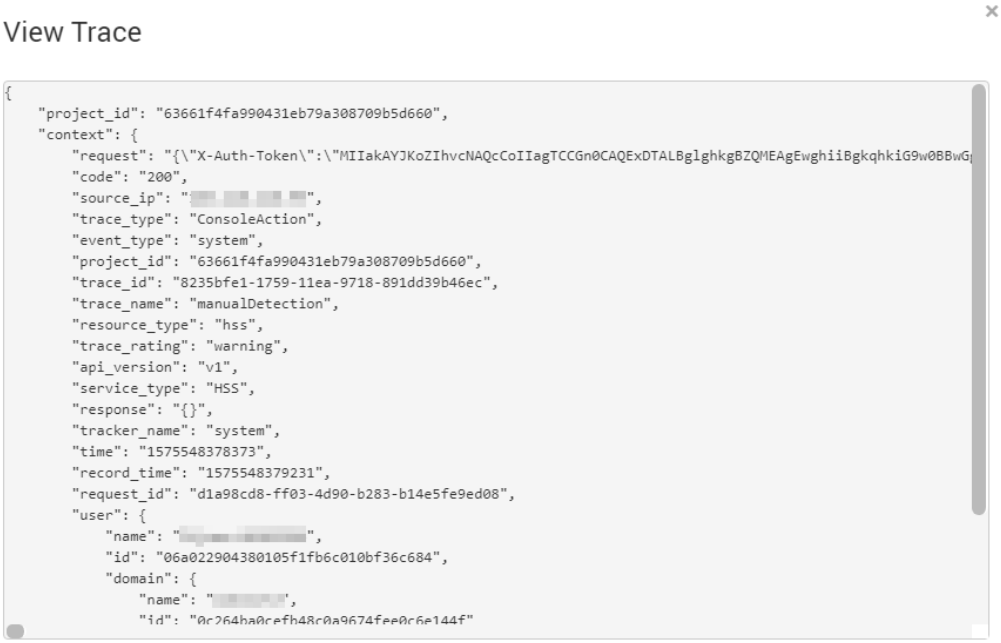
Step 6 Click ⌄ on the left of a trace to expand its details, as shown in **Figure 13-1**.

Figure 13-1 Expanding trace details



Step 7 Click **View Trace** in the **Operation** column. On the displayed **View Trace** dialog box shown in **Figure 13-2**, the trace structure details are displayed.

Figure 13-2 Viewing a trace



----End

14 Permissions Management

14.1 Creating a User and Granting Permissions

This section describes IAM's fine-grained permissions management for your DEW resources. With **IAM**, 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 HSS 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 on your HSS resources.

If your HUAWEI CLOUD account does not require individual IAM users, skip this chapter.

This section describes the procedure for granting permissions (see **Figure 14-1**).

Prerequisites

Before authorizing permissions to a user group, you need to know which HSS permissions can be added to the user group. **Table 14-1** describes the policy details.

 Copyright © Huawei Technologies Co., Ltd.

Table 14-1 System-defined permissions supported by HSS

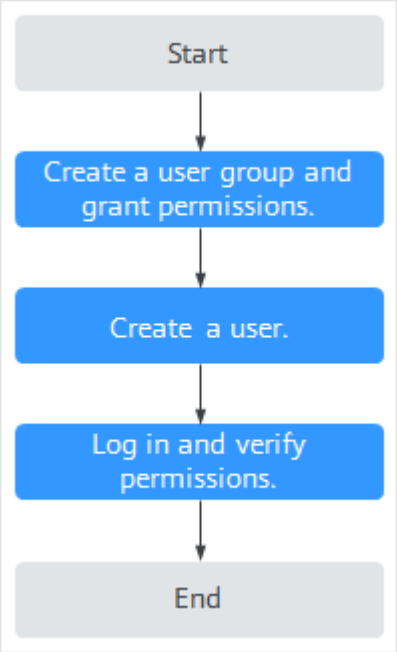
Role/Policy Name	Description	Role/ Policy Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS.	System-defined role	• This role depends on the **Tenant Guest** role. **Tenant Guest**: a global role, which must be assigned in the Global project • To purchase HSS protection quotas, you must have the **ECS ReadOnlyAccess** and **BSS Administrator** roles. – **ECS ReadOnlyAccess**: read-only access permission for the ECS. This is a system policy. – **BSS Administrator**: a system role, which is the administrator of the billing center (BSS) and has all permissions for the service.
HSS FullAccess	Full permissions for HSS	System-defined policy	To purchase HSS protection quotas, you must have the **BSS Administrator** role. **BSS Administrator**: a system role, which is the administrator of the billing center (BSS) and has all permissions for the service.

 Copyright © Huawei Technologies Co., Ltd.

Role/Policy Name	Description	Role/ Policy Type	Dependency
HSS ReadOnlyAccess	Read-only permissions for HSS	System-defined policy	None

Process Flow

Figure 14-1 Process for granting permissions



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

   Create a user group on the IAM console and grant the user group the **HSS Administrator** permission for HSS.

2. **Create an IAM user**.

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

3. **Log in** and verify permissions.

   Log in to the HSS console by using the created user, and verify that the user only has read permissions for HSS.

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

 Copyright © Huawei Technologies Co., Ltd.

14.2 HSS Custom Policies

Custom policies can be created to supplement the system-defined policies of HSS. For details about the actions supported by custom policies, see **Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common HSS custom policies.

Example Custom Policies

- Example 1: Allowing users to query the protected server list

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "hss:hosts:list"
                                ]
        }
    ]
}
```

- Example 2: Denying agent uninstallation

  A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **HSS Administrator** policy to a user but also forbid the user from deleting key pairs (**hss:agent:uninstall**). Create a custom policy with the action to delete key pairs, set its **Effect** to **Deny**, and assign both this and the **HSS Administrator** policies to the group the user belongs to. Then the user can perform all operations on HSS except uninstalling it. The following is an example policy that denies agent uninstallation.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "hss:agent:uninstall"
            ]
        },
    ]
}
```

- Multi-action policy

  A custom policy can contain the actions of multiple services that are of the project-level type. The following is an example policy containing actions of multiple services:

```
{
    "Version": "1.1",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "hss:hosts:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "hss:hosts:switchVersion",
                "hss:hosts:manualDetect",
                "hss:manualDetectStatus:get"
            ]
        }
    ]
}
```

14.3 Actions

This section describes fine-grained permissions management for your HSS instances. If your HUAWEI CLOUD account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using **roles** and **policies**. Roles are provided by IAM to define service-based permissions depending on user's job responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

Supported Actions

DNS provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Actions supported by policies are specific to APIs. Common concepts related to policies include:

- Permission: A statement in a policy that allows or denies certain operations.
- Action: Specific operations that are allowed or denied.
- Dependent actions: When assigning an action to users, you also need to assign dependent permissions for that action to take effect.
- IAM projects or enterprise project: Scope of users a permission is granted to. Policies that contain actions for both IAM and enterprise projects can be used and take effect for both IAM and Enterprise Management. Policies that only contain actions supporting IAM projects can be assigned to user groups and only take effect in IAM. Such policies will not take effect if they are assigned to user groups in Enterprise Management.

NOTE

√: supported; x: not supported

A range of HSS actions can be defined in custom policies.

Actions

Permission	Action	Dependent Permission	IAM Project	Enterprise project
Query the protected server list	hss:hosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list	√	√
Enable or disable protection on servers	hss:hosts:switchVersion	-	√	√
Manual scan	hss:hosts:manualDetect	-	√	√
Check the status of a manual scan	hss:manualDetectStatus:get	-	√	√
Query weak password scan reports	hss:weakPwds:list	-	√	√
Query account cracking protection reports	hss:accountCracks:list	-	√	√
Unblock an IP address that was blocked during account cracking prevention	hss:accountCracks:unblock	-	√	√
Query malicious program scan results	hss:maliciousPrograms:list	-	√	√
Query remote login scan results	hss:abnorLogins:list	-	√	√
Query important file change reports	hss:keyfiles:list	-	√	√

Copyright © Huawei Technologies Co., Ltd.

Permission	Action	Dependent Permission	IAM Project	Enterprise project
Query the open port list	hss:ports:list	-	√	√
Query the vulnerability list	hss:vuls:list	-	√	√
Perform batch operations on vulnerabilities	hss:vuls:operate	-	√	√
Query the account list	hss:accounts:list	-	√	√
Query the software list	hss:softwares:list	-	√	√
Query the web path list	hss:webdirs:list	-	√	√
Query the process list	hss:processes:list	-	√	√
Query configuration scan reports	hss:configDetects:list	-	√	√
Query web shell scan results	hss:webshells:list	-	√	√
Query risky account scan reports	hss:riskyAccounts:list	-	√	√
Obtain server risk statistics	hss:riskyDashboard:get	-	√	√
Query password complexity policy scan reports	hss:complexityPolicys:list	-	√	√

Copyright © Huawei Technologies Co., Ltd.

Permission	Action	Dependent Permission	IAM Project	Enterprise project
Perform batch operations on malicious programs	hss:maliciousPrograms:operate	-	√	√
Perform batch operations on open ports	hss:ports:operate	-	√	√
Perform operations on detected unsafe settings	hss:configDetects:operate	-	√	√
Perform batch operations on web shells	hss:webshells:operate	-	√	√
Set common login locations	hss:commonLocations:set	-	√	√
Query common login locations	hss:commonLocations:list	-	√	√
Set common login IP addresses	hss:commonIPs:set	-	√	√
Query common login IP addresses	hss:commonIPs:list	-	√	√
Set the login IP address whitelist	hss:whiteIps:set	-	√	√
Query the login IP address whitelist	hss:whiteIps:list	-	√	√

Copyright © Huawei Technologies Co., Ltd.

Permission	Action	Dependent Permission	IAM Project	Enterprise project
Set weak passwords	hss:weakPwds:set	-	√	√
Query weak passwords	hss:weakPwds:get	-	√	√
Set web paths	hss:webDirs:set	-	√	√
Query web paths	hss:webDirs:get	-	√	√
Obtain the list of servers where 2FA is enabled	hss:twofactorAuth:list	-	√	√
Set 2FA	hss:twofactorAuth:set	-	√	√
Enable or disable automatic isolation and killing of malicious programs	hss:automaticKillMp:set	-	√	√
Query the programs that have been automatically isolated and killed	hss:automaticKillMp:get	-	√	√
Subscribe to security reports	hss:safetyReport:set	-	√	√
Query security reports	hss:safetyReport:list	-	√	√
Query yearly/monthly quota	hss:quotas:get	-	√	√
Purchase quota	hss:quotas:set	-	√	√

Copyright © Huawei Technologies Co., Ltd.

Permission	Action	Dependent Permission	IAM Project	Enterprise project
Query the agent download address	hss:installAgent:get	-	√	√
Uninstall the agent	hss:agent:uninstall	-	√	√
Query HSS alarms	hss:alertConfig:get	-	√	√
Set HSS alarms	hss:alertConfig:set	-	√	√
Query the WTP list	hss:wtpHosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list	√	√
Enable or disable WTP	hss:wtpProtect:switch	-	√	√
Set backup servers	hss:wtpBackup:set	-	√	√
Query backup servers	hss:wtpBackup:get	-	√	√
Set protected directories	hss:wtpDirectorys:set	-	√	√
Query the protected directory list	hss:wtpDirectorys:list	-	√	√
Query WTP records	hss:wtpReports:list	-	√	√
Set privileged processes	hss:wtpPrivilegedProcess:set	-	√	√
Query the privileged process list	hss:wtpPrivilegedProcesses:list	-	√	√
Set a protection mode	hss:wtpProtectMode:set	-	√	√

Copyright © Huawei Technologies Co., Ltd.

Permission	Action	Dependent Permission	IAM Project	Enterprise project
Query the protection mode	hss:wtpProtectMode:get	-	√	√
Set a protected file system	hss:wtpFilesystems:set	-	√	√
Query the protected file system list	hss:wtpFilesystems:list	-	√	√
Set scheduled protection	hss:wtpScheduledProtections:set	-	√	√
Query scheduled protection	hss:wtpScheduledProtections:get	-	√	√
Setting WTP alarms	hss:wtpAlertConfig:set	-	√	√
Query WTP alarms	hss:wtpAlertConfig:get	-	√	√
Query WTP statistics	hss:wtpDashboard:get	-	√	√
Query policy group	hss:policy:get	-	√	√
Set policy group	hss:policy:set	-	√	√
Query Application Recognition Service (ARS)	hss:ars:get	-	√	√
Set ARS	hss:ars:set	-	√	√
Query the detected intrusion list	hss:event:get	-	√	√
Perform operations on intrusions	hss:event:set	-	√	√

Copyright © Huawei Technologies Co., Ltd.

Permission	Action	Dependent Permission	IAM Project	Enterprise project
Query server groups	hss:hostGroup:get	-	√	√
Set server groups	hss:hostGroup:set	-	√	√
Monitor file integrity	hss:keyfiles:set	-	√	√
Query important file change reports	hss:keyfiles:list	-	√	√
Query the auto-startup list	hss:launch:list	-	√	√

Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2022-05-26	This is the thirty-fourth official release. Added the Agent upgrade instructions.
2022-04-25	This is the thirty-third official release. Added/Modified the following content: ● Description of the basic edition and its capabilities ● Description of whitelist configuration ● Description that alarms do not indicate successful intrusions
2022-01-27	This is the thirty-second official release. Added the following sections: **HSS Operations Supported by CTS** **Viewing Audit Logs**
2021-12-30	This is the thirty-first official release. Modified the following content: Added the description about Message Center and SMN topic settings in **(Optional) Step 3: Set Alarm Notifications**. Added the description about the maximum number of mobile numbers or email addresses in **Security Configuration**. Added the description about the scenario of the basic edition in **Step 1: Purchase HSS Quota**. Deleted description about the upgrade to the Web Tamper Protection edition in **Upgrading a Quota**.
2021-08-03	This issue is the thirtieth official release. ● Optimized descriptions in **Step 1: Purchase HSS Quota**. ● Added the description about configuring the SSH login whitelist and 2FA constraints in **Security Configuration**.

 Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2021-07-14	This is the twenty-ninth official release. ● Optimized descriptions in **Step 1: Purchase HSS Quota**. ● Optimized descriptions in **Enabling the Basic/Enterprise/Premium Edition**.
2021-06-08	This is the twenty-eighth official release. ● Added the open port check time in **Asset Management**. ● Added the vulnerability patch update time in **Viewing Details of a Vulnerability**.
2021-05-08	This is the twenty-seventh official release. In **Installing an Agent on the Windows OS**, the link for downloading the agent package was added to the console. Users can copy the link and log in to the server to download the package using Internet Explorer.
2021-02-25	This is the twenty-sixth official release. Modified description in **(Optional) Step 3: Set Alarm Notifications**, allowing you to enable HSS without enabling alarm notifications.
2021-01-26	This is the twenty-fifth official release. Added **(Optional) Step 5: Switching the HSS Edition**.
2020-12-29	This is the twenty-fourth official release. Added Linux ransomware protection in **Ransomware Prevention**.
2020-12-24	This issue is the twenty-third official release. Added the description about searching for a server by its protection billing mode or server billing mode in **Viewing the Server List**.
2020-12-08	This is the twenty-second official release. Added **Managing Quotas**.
2020-11-16	This is the twenty-first official release. Cross-region usage is not supported in **Installing an Agent on the Linux OS** and **Installing an Agent on the Windows OS**.
2020-10-15	This is the twentieth official release. ● Added the description of alarm notification items in **Enabling the Basic/Enterprise/Premium Edition**. ● Added the path for monitoring key files in **Alarm Events**. ● Added alarm handling suggestions in **Checking and Handling Intrusion Events**.
2020-09-21	This is the nineteenth official release. Added **Managing All Projects Settings**.

Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2020-06-19	This is the eighteenth official release. ● Added **Application Recognition Service**. ● Added **Ransomware Prevention**. ● Added **Managing Projects and Enterprise Projects**. ● Added the description about enterprise project options in **Step 1: Purchase HSS Quota**. ● Added the function of searching for servers by server status in **Viewing the Server List**.
2020-06-05	This issue is the seventeenth official release. ● Added description about how to bind a quota to a server to enable protection, and about how to unbind a quota from a server in **Step 4: Enable Server Protection**. ● Added description about using the recipient settings in the Message Center in **Enabling the Basic/Enterprise/Premium Edition**. ● Added the one-click fix and verification functions in **Fixing Vulnerabilities and Verifying the Result**.
2020-05-18	This issue is the sixteenth official release. ● Added support for advanced search in **Viewing the Server List**. ● Added description about how to import and export the alarm whitelist in **Configuring the Alarm Whitelist**. ● Changed the file integrity check function to file integrity monitoring in **File Integrity Monitoring**. ● The premium edition is provided free of charge for users who have purchased the WTP edition.

Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2020-04-09	This is the fifteenth official release. Added the following section: • **Creating a Server Group** • **Applying a Policy** • **Checking and Handling Intrusion Events** • **Managing Isolated Files** • **Configuring the Alarm Whitelist** • **Configuring the Login Whitelist** • Application Recognition Service • Critical File Check • **Checking or Creating a Policy Group** • **Modifying a Policy** • **HSS Custom Policies** • **Actions**
2019-12-18	This is the fourteenth official release. • Modified section **Security Configuration**. Added description about the support for IPv6 addresses in the SSH login IP address whitelist. • Added section **Subscribing to HSS Reports**.
2019-09-04	This is the thirteenth official release. Updated the content structure.
2019-08-09	This is the twelfth official release. Non-HUAWEI CLOUD servers are supported.
2019-07-19	This is the eleventh official release. Optimized the structure of the document to provide users with better reference.
2019-07-03	This is the tenth official release. Updated screenshots.
2019-03-28	This is the ninth official release. Updated the screenshots and related descriptions in section **Adding a Protected Directory or File System**.
2019-02-28	This is the eighth official release. Updated screenshots.
2019-01-17	This is the seventh official release. Updated screenshots.

Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2018-11-29	This is the sixth official release. ● Updated the screenshots and related descriptions in section **Enabling Alarm Notification**. ● Updated screenshots and related descriptions in section **Security Configuration**.
2018-10-25	This is the fifth official release. Updated screenshots and related descriptions in section **Dashboard**.
2018-09-27	This is the fourth official release. ● Updated screenshots and related descriptions in section **Vulnerability Management**. ● Updated the screenshots and related descriptions in section **Asset Management**.
2018-09-15	This is the third official release. ● Updated screenshots in section **Intrusion Detection**. ● Updated the screenshots and related descriptions in section **Asset Management**. ● Updated the screenshots and related descriptions in section **Baseline Inspection**.
2018-08-30	This is the second official release. Added "Malicious Programs Detection".
2018-08-16	This is the first official release.

Copyright © Huawei Technologies Co., Ltd.