Host Security Service

User Guide

Issue	21
Date	2024-03-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

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

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Accessing HSS

1.1 Access Guide

Figure 1-1 shows the process of accessing HSS.

Figure 1-1 HSS access process

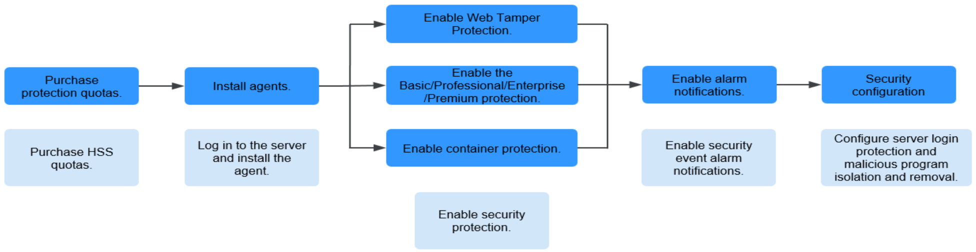

Purchase protection quotas.
Purchase HSS quotas.
Install agents.
Log in to the server and install the agent.
Enable Web Tamper Protection.
Enable the Basic/Professional/Enterprise /Premium protection.
Enable container protection.
Enable security protection.
Enable alarm notifications.
Enable security event alarm notifications.
Security configuration
Configure server login protection and malicious program isolation and removal.

Table 1-1 Description of the HSS access process

No.	Step	Description
1	**Purchasing Protection Quotas**	HSS provides the basic, professional, enterprise, premium, web tamper protection, and container edition. Each edition supports different functions and features. You need to purchase the corresponding edition based on your protection requirements for servers or containers. For details about the differences between HSS versions, see **Specifications of Different Editions**.
2	**Installing the Agent**	The HSS agent is a piece of software installed on cloud servers to exchange data between the servers and HSS, implementing security detection and protection. You can use only after installing the agent.
3	**Enabling Protection**	You need to enable protection for your ECSs.

No.	Step	Description
4	**Enabling Alarm Notifications**	By default, security risks detected by HSS are displayed on the management console. You need to log in to the console and view the risks. If you want to know the security risks of servers or containers in a timely manner, you can enable the alarm notification function. After the function is enabled, HSS will send security risks to you by SMS or email.
5	**Common Security Configurations**	To improve ECS security, you can configure the following ECS security protection items based on your service requirements: ● Common login locations: HSS allows users to log in to ECSs in common login locations and generates alarms when users log in to ECSs in non-common login locations. ● Common login IP address: HSS allows common login IP addresses to log in to ECSs and generates alarms for uncommon login IP addresses. ● SSH login IP address whitelist: HSS only allows IP addresses in the whitelist to log in to ECSs using SSH. ● Two-factor authentication: The two-factor authentication mechanism is used together with the SMS or email verification code to perform secondary authentication on ECS login. ● Isolation and killing of malicious programs: HSS automatically isolates and kills identified malicious programs, such as backdoors, Trojans, and worms.

1.2 Purchasing Quota

You can purchase an HSS quota on the console.

Precautions

- The quota can be used only in the region where you bought it.
- A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- Currently, HSS can only protect Docker and Containerd containers. Check your container type before purchasing the container edition.
- HSS should be deployed 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.
- After purchasing quota, go to the **Servers & Quota** page to enable HSS.
- The premium edition is provided for free if you have purchased the WTP edition.

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, the HSS enterprise edition stops charging if the servers it protects are stopped.

Regions

Table 1-2 Choosing a region to purchase HSS

Server	Server Region	Region
ECS BMS HECS Huawei Cloud Workspace	Regions where HSS is available	Regions where your ECSs/BMSs/HECSs/Workspaces are deployed HSS cannot be used across regions. If the server and your protection quota are in different regions, unsubscribe from the quota and purchase a quota in the region where the server is deployed.
Third-party cloud server	-	Currently, only some regions support access to non-Huawei Cloud servers. For details about the regions, see **Where Is HSS Available?** Purchase an HSS quota in the region that supports non-Huawei Cloud servers. Connect the server to the region by performing the installation procedure for non-Huawei Cloud servers.
Offline server	-	

Prerequisites

The account must have the **BSS Administrator** and **HSS Administrator** permissions. If the account does not have the permissions, use a master account to purchase quotas or authorize member accounts to purchase quotas.

Procedure

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

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **HSS** to go to the HSS management console.

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.

Table 1-3 Parameters for purchasing HSS

Parameter	Description	Example Value
Billing Mode	Select **Yearly/Monthly** or **Pay-per-use** billing mode based on your requirements. ● Yearly/Monthly: You can select the basic, professional, enterprise, premium, WTP, or container edition. You can purchase the edition for a fixed period of time. The fee is 30% lower than that of pay-per-use. If you use the edition for a long time, you are advised to purchase yearly/monthly packages. ● Pay-per-use: Only the enterprise edition can be purchased. You need to enable this edition in the server list. You pay for the duration you use the resources. Prices are calculated by hour, and no minimum fee is required. **NOTE** Procedure for enabling pay-per-use quota: 1. On the purchase page, select **Pay-per-use**. The **Enterprise** edition will be automatically selected. In the lower right corner, click **Enable Now**. You will be redirected to the server list. 2. In the server list, click **Enable** in the **Operation** column. Set the **Billing Mode** to **Pay-per-use** and **Edition** to **Enterprise**. 3. Confirm the information and click **OK**.	Yearly/ Monthly
Region	● To minimize connection issues, purchase quota in the region of your servers.	CN-Hong Kong
Edition	The **basic, professional, enterprise,premium,WTP,** and **container editions** are supported. For details about the differences between editions, see **Editions**. **NOTICE** ● If you enable the HSS basic edition for the first time, you can enjoy the free trial for 30 days and purchase it after the trial. ● If you purchased the basic, enterprise, or premium edition, enable it on the **Asset Management** > **Servers & Quota** page. ● If you purchased the WTP edition, enable it in the server list on the **Prevention** > **Web Tamper Protection** page. ● If you purchased the container edition, choose **Asset Management** > **Containers & Quota** and enable protection on the **Container Nodes** tab.	Enterprise

Parameter	Description	Example Value
Enterprise Project	This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects. 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. Select an enterprise project from the drop-down list. **NOTE** ● Resources and incurred expenses are managed under the enterprise project you selected. ● 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. ● The **default** option is available in the **Enterprise Project** drop-down list only after you purchased HSS under your Huawei ID.	default
Required duration	● Select a duration based on your requirements. In **Pay-per-use** mode, you do not need to select a duration. ● 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.	1 year
Server Quota	Enter the number of HSS quotas to be purchased. In **Pay-per-use** mode, you do not need to configure this option. **NOTICE** ● All your servers should be protected, so that if a virus (such as ransomware or a mining program) infects one of them, it will not be able to spread to others and damage your entire network. ● You cannot modify the quota of an edition after its purchase is complete. You can unsubscribe from it and purchase again.	20
Tag	Tags are used to identify cloud resources. When you have many cloud resources of the same type, you can use tags to classify cloud resources by dimension (for example, by usage, owner, or environment). To use this function, your account must have the **TMS administrator** permission. Without this permission, you cannot add tags to protection quotas, and the error message "permission error" will be displayed. You do not need to set this parameter in pay-per-use mode.	data

Parameter	Description	Example Value
Quota Management	After automatic quota binding is enabled, HSS automatically binds available quotas to new servers or container nodes after the agent is installed for the first time. Only the yearly/monthly quotas that you have purchased can be automatically bound. No new order or fee is generated. ● Servers: Available yearly/monthly quotas are automatically bound in the following sequence: Premium Edition > Enterprise Edition > Professional Edition > Basic Edition. ● Container nodes: Available yearly/monthly quotas are automatically bound in the following sequence: Container Edition > Premium Edition > Enterprise Edition > Professional Edition > Basic Edition.	Selected

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 Now** and complete the payment.

----End

Follow-up Procedure

After purchasing the quota, you need to install the agent for server and enable it. For details, see **Installing an Agent** and **Enabling Protection**.

Related Operations

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

1.3 Installing an Agent

1.3.1 Agent Overview

What is an agent?

The HSS agent is a piece of software installed on cloud servers to exchange data between the servers and HSS, implementing security detection and protection. If no agent is installed, the HSS is unavailable.

Scans all servers at 00:00 every day; monitors the security and monitors status of servers; and reports the collected server and monitors information (including non-compliant configurations, insecure configurations, intrusion traces, software list, port list, and process list) to the cloud protection center. In addition, the agent blocks attacks targeted at servers and containers based on the security policies you configured.

Supported OSs

Currently, some mainstream OSs are supported. For details, see **Supported OSs**. To obtain better HSS service experience, you are advised to install or upgrade to an OS version supported by the agent.

Processes When the Agent Is Running

- **Linux**

  The account of the agent is **root**. **Table 1-4** lists the running processes on a Linux server.

Table 1-4 Agent running process on a Linux server

Agent Process Name	Function	Path
hostguard	Detects security issues, protects the system, and monitors the agent.	/usr/local/hostguard/bin/hostguard
hostwatch	Monitors the agent process.	/usr/local/hostguard/bin/hostwatch
upgrade	Upgrades the agent.	/usr/local/hostguard/bin/upgrade

- **Windows**

  The account of the agent is **system**. **Table 1-5** lists the running processes on a Windows server.

Table 1-5 Agent running process on a Windows server

Agent Process Name	Function	Path
hostguard.exe	Detects security issues, protects the system, and monitors the agent.	C:\Program Files\HostGuard\HostGuard.exe
hostwatch.exe	Monitors the agent process.	C:\Program Files\HostGuard\HostWatch.exe
upgrade.exe	Upgrades the agent.	C:\Program Files\HostGuard\upgrade.exe

Installing an Agent

- **Installing the Agent on a Linux Server**
- **Installing the Agent on a Windows Server**
- **Installing the Agent on Linux Servers in Batches**

1.3.2 Installing the Agent on a Linux Server

You can enable HSS for ECSs only after installing the agent. This section describes how to install the agent on a Linux server.

Prerequisites

- The ECS is in the **Running** state and can access the Internet.
- Ensure the outbound rule of your security group allows access to the port 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- The DNS server address of the cloud server has been set to the private DNS server address. For details, see **Changing the DNS Server Address of an ECS** and **Private DNS Server Addresses**.
- The available capacity of the disk where the agent is installed must be greater than 300 MB. Otherwise, the agent installation may fail.
- The Security-Enhanced Linux (SELinux) firewall has been disabled. The firewall affects agent installation and should remain disabled until the agent is installed.
- If any third-party security software has been installed on your server, the HSS agent may fail to be installed. In this case, disable or uninstall the software before installing the agent.

Constraints

- 64-bit Huawei Cloud servers and non-Huawei Cloud servers can be protected. 32-bit servers are no longer supported.
- Mainstream OSs are supported. For details, see **Supported OSs**.
- The HSS agent will be automatically installed on Workspace 23.6.0 or later. If your Workspace version is earlier than 23.6.0, you can manually install the agent by referring to this section.

Installation Path

The agent installation path on servers running on Linux cannot be customized. The default path is: **/usr/local/hostguard/**.

Installation Operations

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** > **HSS**.

Step 3 In the navigation pane, choose **Installation & Configuration**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Agent Management** tab.

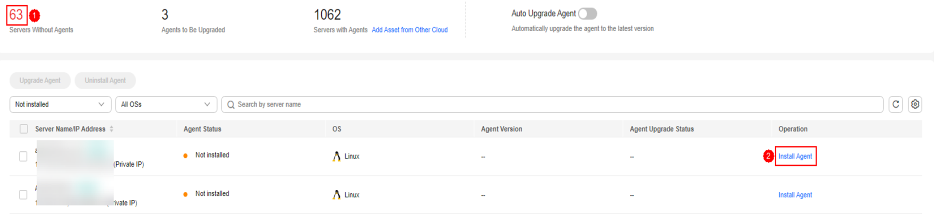
Step 5 Copy the command for installing the agent.

- Huawei Cloud server

  a. Click the value in the **Servers Without Agents** area to filter the servers where the agent is not installed.

  b. In the **Operation** column of a server, click **Install Agent**.

  Figure 1-2 Installing an agent



Server Name/IP Address	Agent Status	OS	Agent Version	Agent Upgrade Status	Operation
[redacted] (Private IP)	Not installed	Linux	--	--	Install Agent
[redacted] rivate IP)	Not installed	Linux	--	--	Install Agent

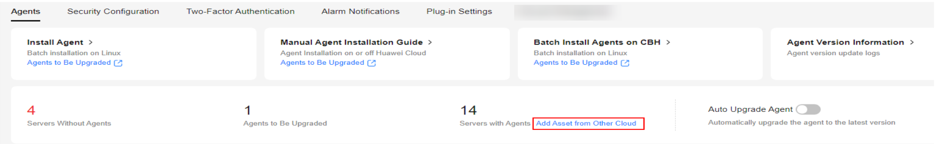
  c. In the displayed dialog box, click **Copy**.

- Non-Huawei Cloud server

  NOTE

  a. Click **Add Asset from Other Cloud**.

  Figure 1-3 Adding asset from other cloud


Agents
Security Configuration
Two-Factor Authentication
Alarm Notifications
Plug-in Settings
Install Agent >
Batch installation on Linux
Agents to Be Upgraded
Manual Agent Installation Guide >
Agent Installation on or off Huawei Cloud
Agents to Be Upgraded
Batch Install Agents on CBH >
Batch installation on Linux
Agents to Be Upgraded
Agent Version Information >
Agent version update logs
4
Servers Without Agents
1
Agents to Be Upgraded
14
Servers with Agents
Add Asset from Other Cloud
Auto Upgrade Agent
Automatically upgrade the agent to the latest version

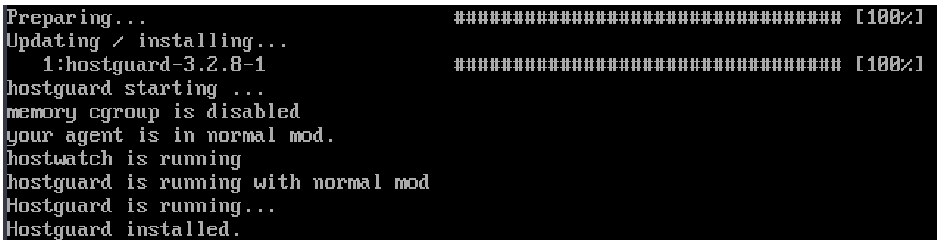
  b. In the displayed slide-out panel, copy the agent installation link suitable for your system OS.

Step 6 Remotely log in to the server where the agent is to be installed.

Step 7 Paste the copied installation command and run it as user **root** to install the agent on the servers.

If the command output shown in **Installation completed** is displayed, the agent is successfully installed.

Figure 1-4 Installation completed



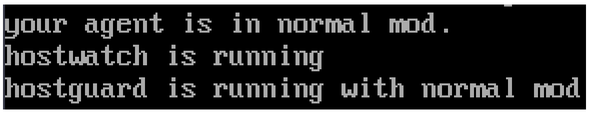
```
Preparing...                          ################################# [100%]
Updating / installing...
   1:hostguard-3.2.8-1                ################################# [100%]
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
Hostguard is running...
Hostguard installed.
```

Step 8 Run the following command to check the runtime status of agent:

service hostguard status

If the command output shown in **Agent running properly** is displayed, the agent is running properly.

Figure 1-5 Agent running properly



```
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
```

After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the **Servers** tab of the **Asset Management** > **Servers & Quota** page.

----End

Follow-up Procedure

After the agent is installed, enable security protection for your server. For details, see **Enabling Protection**.

FAQs

- For details about the agent status and troubleshooting, see **How Do I Fix an Abnormal Agent?**
- 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?**

1.3.3 Installing the Agent on a Windows Server

You can enable HSS for ECSs only after installing the agent. This section describes how to install the agent on a Windows server.

Prerequisites

- The ECS is in the **Running** state and can access the Internet.
- Ensure the outbound rule of your security group allows access to the port 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- The DNS server address of the cloud server has been set to the private DNS server address. For details, see **Changing the DNS Server Address of an ECS** and **Private DNS Server Addresses**.
- The available capacity of the disk where the agent is installed must be greater than 300 MB. Otherwise, the agent installation may fail.
- The Security-Enhanced Linux (SELinux) firewall has been disabled. The firewall affects agent installation and should remain disabled until the agent is installed.
- If any third-party security software has been installed on your server, the HSS agent may fail to be installed. In this case, disable or uninstall the software before installing the agent.

Constraints

- 64-bit Huawei Cloud servers and non-Huawei Cloud servers can be protected. 32-bit servers are no longer supported.
- Mainstream OSs are supported. For details, see **Supported OSs**.
- The HSS agent will be automatically installed on Workspace 23.6.0 or later. If your Workspace version is earlier than 23.6.0, you can manually install the agent by referring to this section.

Installation Path

The agent installation path on servers running on Windows cannot be customized. The default path is: **C:\Program Files\HostGuard**.

Installation Operations

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

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **HSS** to go to the HSS management console.

Step 3 In the navigation pane, choose **Installation & Configuration**.

NOTE

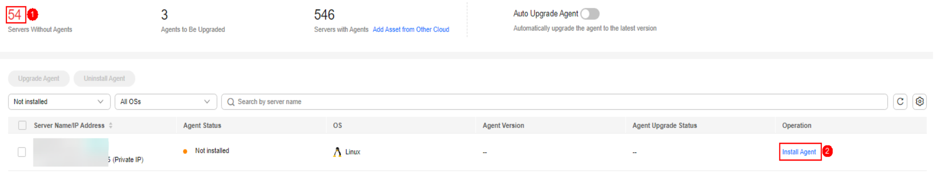
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the **Agent Management** tab.

Step 5 Copy the address for downloading the agent installation package.

- Huawei Cloud server
  a. Click the value in the **Servers Without Agents** area to filter the servers where the agent is not installed.
  b. In the **Operation** column of a server, click **Install Agent**.

Figure 1-6 Installing an agent



Server Name/IP Address	Agent Status	OS	Agent Version	Agent Upgrade Status	Operation
[redacted] 5 (Private IP)	Not installed	Linux	--	--	Install Agent

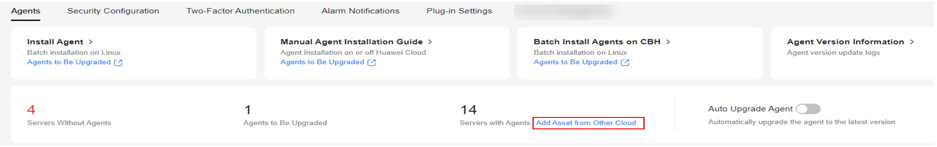
  c. In the displayed dialog box, click **Copy** to copy the address for downloading the agent installation package.

- Non-Huawei Cloud server

  NOTE

  a. Click **Add Asset from Other Cloud**.

Figure 1-7 Adding asset from other cloud


Agents
Security Configuration
Two-Factor Authentication
Alarm Notifications
Plug-in Settings
Install Agent >
Batch installation on Linux
Agents to Be Upgraded
Manual Agent Installation Guide >
Agent Installation on or off Huawei Cloud
Agents to Be Upgraded
Batch Install Agents on CBH >
Batch installation on Linux
Agents to Be Upgraded
Agent Version Information >
Agent version update logs
4
Servers Without Agents
1
Agents to Be Upgraded
14
Servers with Agents
Add Asset from Other Cloud
Auto Upgrade Agent
Automatically upgrade the agent to the latest version

b. In the displayed slide-out panel, copy the address for downloading the agent installation package suitable for your system OS.

Step 6 Remotely log in to the server where the agent is to be installed.

Step 7 On the server where the agent is to be installed, use Internet Explorer to download the agent installation package from the copied agent download address and decompress it.

Step 8 Run the agent installation program as an administrator.

Step 9 Select a host type on the **Select host type** page.

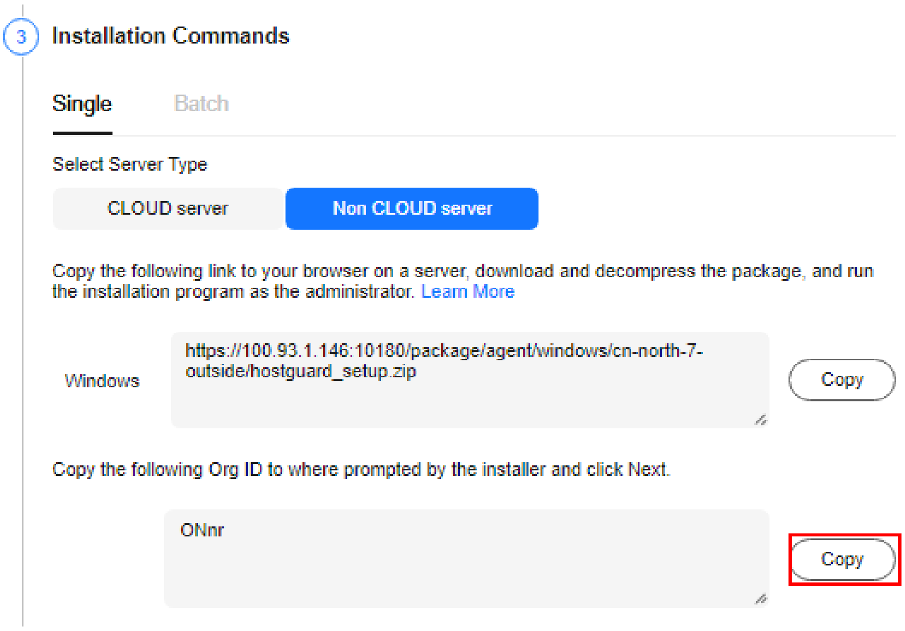
- Huawei Cloud server: Select **Huawei Cloud Host**.
- Non-Huawei Cloud server: Select **Other Cloud Host**.

  Copy Org ID from the agent installation page, as shown in **Obtaining the Org ID (for a non-Huawei Cloud server)**. Enter the Org ID and install the agent as prompted.

NOTICE

Ensure Org ID is correct. Otherwise, the agent status may be displayed as **Not installed** even if the installation succeeded.

Figure 1-8 Obtaining the Org ID (for a non-Huawei Cloud server)



Copy the following link to your browser on a server, download and decompress the package, and run the installation program as the administrator.

https://100.93.1.146:10180/package/agent/windows/cn-north-7-outside/hostguard_setup.zip

Copy the following Org ID to where prompted by the installer and click Next.

ONnr

Step 10 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. It takes 3 to 5 minutes for the console to update the agent status after agent installation.

----End

Follow-up Procedure

After the agent is installed, enable security protection for your server. For details, see **Enabling Protection**.

FAQs

- For details about the agent status and troubleshooting, see **How Do I Fix an Abnormal Agent?**
- 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?**

1.3.4 Installing the Agent on Linux Servers in Batches

HSS allows you to install agents on Linux servers in batches, preventing the installation from taking too much time. Agents cannot be installed on Windows servers in batches.

Prerequisite

- The ECS is in the **Running** state and can access the Internet.
- Ensure the outbound rule of your security group allows access to the port 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- The DNS server address of the cloud server has been set to the private DNS server address. For details, see **Changing the DNS Server Address of an ECS** and **Private DNS Server Addresses**.
- The available capacity of the disk where the agent is installed must be greater than 300 MB. Otherwise, the agent installation may fail.
- The Security-Enhanced Linux (SELinux) firewall has been disabled. The firewall affects agent installation and should remain disabled until the agent is installed.
- If any third-party security software has been installed on your server, the HSS agent may fail to be installed. In this case, disable or uninstall the software before installing the agent.
- The server supports SSH login.

Constraints

- 64-bit Huawei Cloud servers and non-Huawei Cloud servers can be protected. 32-bit servers are no longer supported.
- Mainstream OSs are supported. For details, see **Supported OSs**.
- The HSS agent will be automatically installed on Workspace 23.6.0 or later. If your Workspace version is earlier than 23.6.0, you can manually install the agent by referring to this section.

Installation Path

The agent installation path on servers running on Linux cannot be customized. The default path is: **/usr/local/hostguard/**.

Installing the Agent on Linux Servers in Batches (One-Click on the Console)

Prerequisite

- There is a server with an online agent in the VPC of the servers where the agent is to be installed. If there is no online agent server, install an agent on a server by referring to **Installing the Agent on a Linux Server**.
- The accounts and passwords of all servers where the agent is to be installed are the same. You have obtained the account, port number, and password for logging in to the servers.

Constraints

You can install the agent on a maximum of 50 servers at a time.

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** > **HSS**.

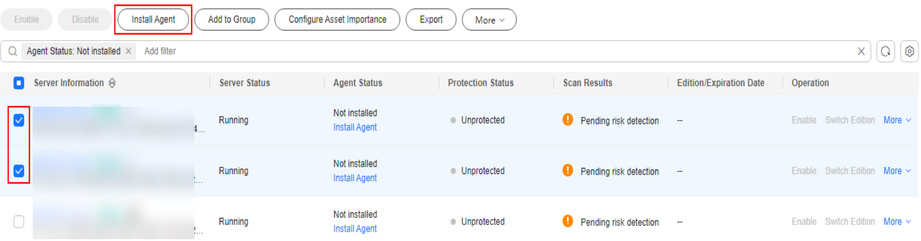
Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Select all target servers and click **Install Agent** above the server list.

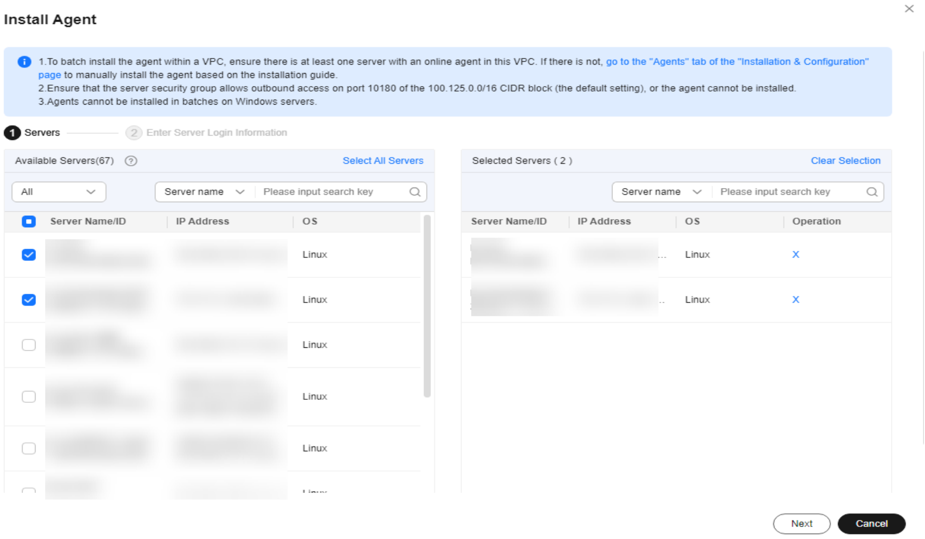
Figure 1-9 Batch installing agents



■ Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Operation
☑ [redacted]	Running	Not installed Install Agent	● Unprotected	! Pending risk detection	--	Enable Switch Edition More
☑ [redacted]	Running	Not installed Install Agent	● Unprotected	! Pending risk detection	--	Enable Switch Edition More
□ [redacted]	Running	Not installed Install Agent	● Unprotected	! Pending risk detection	--	Enable Switch Edition More

Step 5 Confirm the selected server information and click **Next**.

Figure 1-10 Selected servers



Install Agent

1.To batch install the agent within a VPC, ensure there is at least one server with an online agent in this VPC. If there is not, go to the "Agents" tab of the "Installation & Configuration" page to manually install the agent based on the installation guide.
2.Ensure that the server security group allows outbound access on port 10180 of the 100.125.0.0/16 CIDR block (the default setting), or the agent cannot be installed.
3.Agents cannot be installed in batches on Windows servers.

■	Server Name/ID	IP Address	OS
☑	[redacted]	[redacted]	Linux
☑	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux

Server Name/ID	IP Address	OS	Operation
[redacted]	[redacted]	Linux	X
[redacted]	[redacted]	Linux	X

Step 6 Enter the server root password and server login port.

NOTE

- The default system port is **22**. To query the Linux SSH port, remotely log in to the target server and run the following command on the Linux server:

```
cat /etc/ssh/sshd_config | grep Port
```

- If the server password contains the character **$**, enter **\$**.

Step 7 Click **OK**. Agents will be automatically installed on the servers you selected.

Agents will be automatically installed on the servers you selected in sequence. You can choose **Asset Management** > **Servers & Quota** and click the **Servers** tab to view agent status. If the **Agent Status** of a target server changes to **Online**, you can enable protection for the server.

----End

Installing the Agent on Linux Servers in Batches (Using the CLI)

Prerequisite

You have obtained the account, port number, and password for logging in to the server.

Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > HSS to go to the HSS management console.

Step 3 In the navigation pane, choose **Installation & Configuration**.

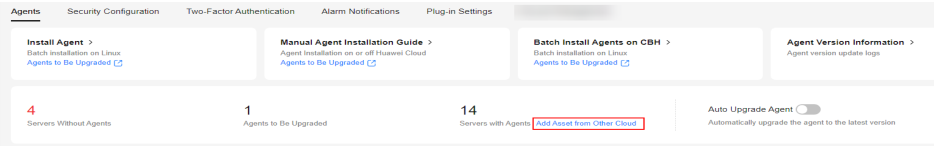
NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the **Agent Management** tab.

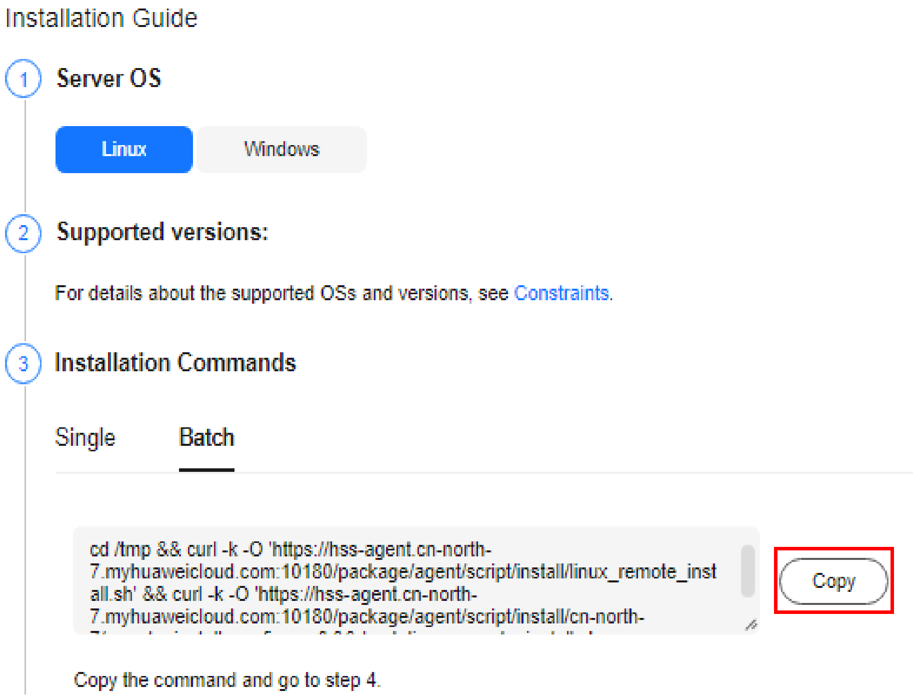
Step 5 Click **Add Asset from Other Cloud**.

Figure 1-11 Adding asset from other cloud


Agents
Security Configuration
Two-Factor Authentication
Alarm Notifications
Plug-in Settings
Install Agent >
Batch installation on Linux
Agents to Be Upgraded
Manual Agent Installation Guide >
Agent Installation on or off Huawei Cloud
Agents to Be Upgraded
Batch Install Agents on CBH >
Batch installation on Linux
Agents to Be Upgraded
Agent Version Information >
Agent version update logs
4
Servers Without Agents
1
Agents to Be Upgraded
14
Servers with Agents
Add Asset from Other Cloud
Auto Upgrade Agent
Automatically upgrade the agent to the latest version

Step 6 In the displayed page, copy the batch installation command.

Figure 1-12 Copying the batch installation command



For details about the supported OSs and versions, see Constraints.

```
cd /tmp && curl -k -O 'https://hss-agent.cn-north-
7.myhuaweicloud.com:10180/package/agent/script/install/linux_remote_inst
all.sh' && curl -k -O 'https://hss-agent.cn-north-
7.myhuaweicloud.com:10180/package/agent/script/install/cn-north-
```

Copy the command and go to step 4.

Step 7 Remotely log in to the server where you plan to install the agent.

NOTICE

After logging in to the server, run the following command to check whether the expect command exists on the server. If the expected command does not exist, configure the yum repository.

/bin/expect -v

Step 8 Run the following command to access the **/tmp** directory:

cd /tmp/

Step 9 Run the following command to create the **linux-host-list.txt** file and add the private IP addresses of the servers you want to install the agent to the file:

- Command format 1: **echo "***IP address Port***root rootPassword" >> linux-host-list.txt**

Example: **echo "127.8.10.8 22 root rootPassword" >> linux-host-list.txt**

- Command format 2: **echo " IP address Port user userPassword rootPassword" >> linux-host-list.txt**

  Example: **echo "127.8.10.9 22 user userPassword rootPassword" >> linux-host-list.txt**

You can use either of the preceding command formats. To specify multiple IP addresses, write multiple commands, each in a separate line.

Example:

echo "127.8.10.1 22 root rootPassword" >> linux-host-list.txt

echo "127.8.10.8 22 root rootPassword" >> linux-host-list.txt

echo "127.8.10.3 22 root rootPassword" >> linux-host-list.txt

Step 10 Press **Enter** to save the IP address and run the following command to check whether the IP address is added:

cat linux-host-list.txt

Step 11 Paste the copied installation command by **6** and run it as user **root** to install the agent on the servers.

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

remote_install finished. [OK]

Step 12 Choose **Installation and Configuration** > **Agents** and check the agent status of the target server. If the agent is online, it is running properly.

Step 13 Run the following command to delete the **linux-host-list.txt** file to prevent password leakage:

rm -rf linux-host-list.txt

----End

1.4 Enabling Protection

1.4.1 Enabling the Basic, Professional, Enterprise, or Premium Edition

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

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

NOTE

To enable the WTP edition, choose **Prevention** > **Web Tamper Protection** > **Server Protection** and click the **Servers** tab. All the functions of the premium edition are included with the WTP edition.

Check Mode

HSS performs a full scan in the early morning every day.

After you enable server protection, you can view scan results after the automatic scan in the next early morning, or perform a **manual scan**.

Prerequisites

- The agent status of the server to be protected is **Online**. To check the status, choose **Asset Management** > **Servers & Quota** on the HSS.
- 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 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **HSS** to go to the HSS management console.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

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 the pay-per-use or yearly/monthly mode.

NOTE

- Only the enterprise edition supports the pay-per-use mode.
- If the quota is insufficient when you select the yearly/monthly mode, you need to purchase HSS quotas.
- If the version of the agent installed on the Linux server is 3.2.10 or later or the version of the agent installed on the Windows server is 4.0.22 or later, ransomware prevention is automatically enabled with the premium edition. Deploy bait files on servers and automatically isolate suspicious encryption processes (there is a low probability that processes are incorrectly isolated). You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Enabling Ransomware Backup**.

- **Yearly/Monthly**

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

  The quotas can be allocated in the following ways:

  – Select **Random quota** to let the system allocate the quota with the longest remaining validity to the server.

  – Select a quota ID and allocate it to a server.

- **Pay-per-use**

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

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, professional, enterprise or premium edition has been enabled.

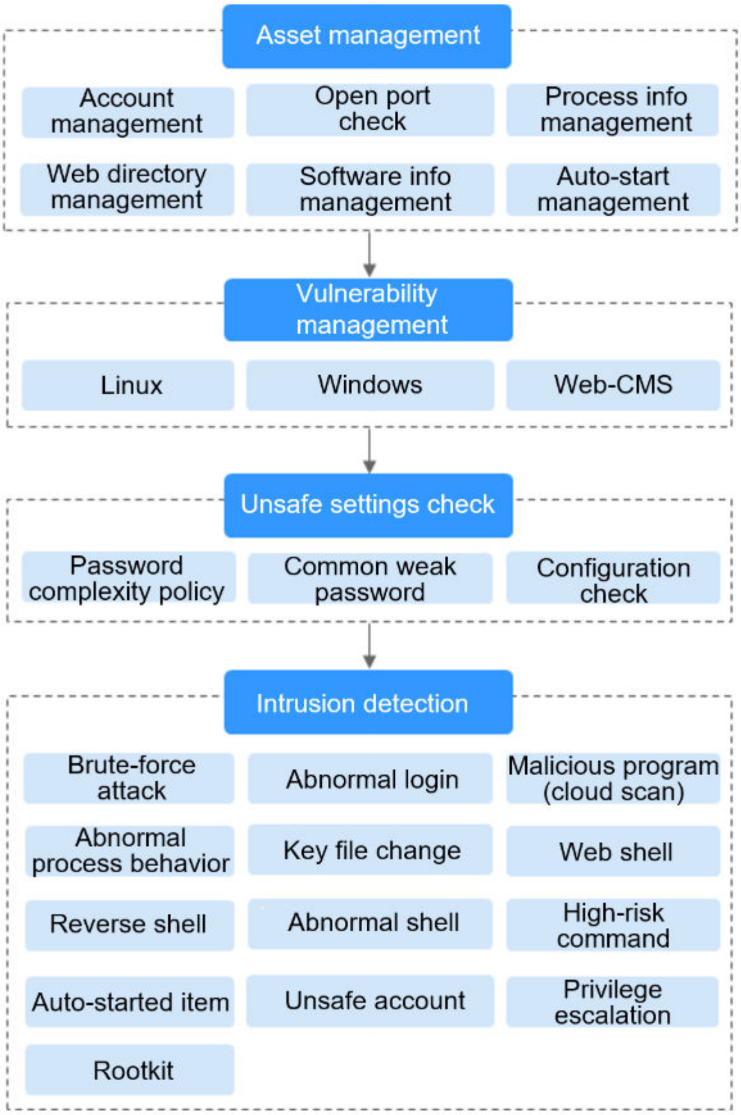
NOTE

- Alternatively, on the **Quotas** tab of the **Servers & Quota** 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.

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

Figure 1-13 Automatic security check items



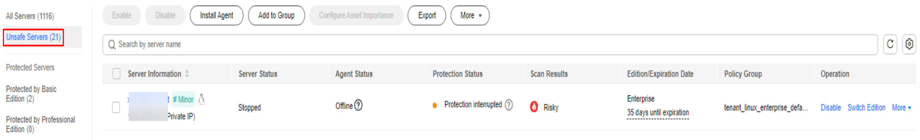
----End

Viewing Detection Details

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

On the left of the protection list, click **Risky Servers**.

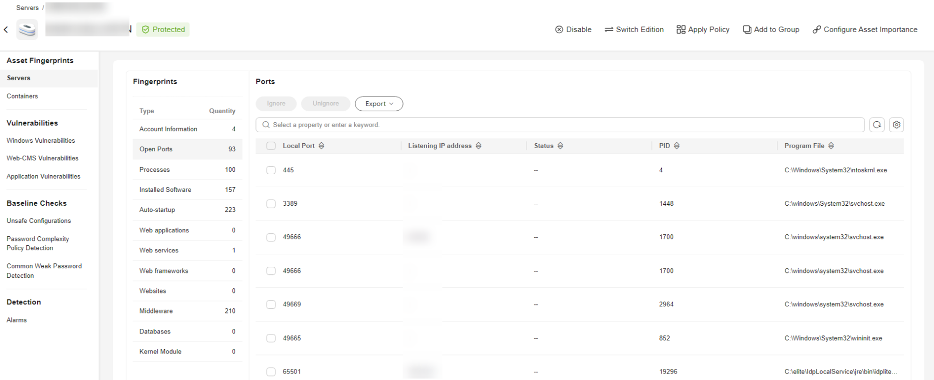
Figure 1-14 Viewing risky items



□ Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Policy Group	Operation
□ [redacted] # Minor Private IP)	Stopped	Offline ?	● Protection interrupted ?	Risky	Enterprise 35 days until expiration	tenant_linux_enterprise_defa...	Disable Switch Edition More ▾

Click a server name to go to the details page. On this page, you can quickly check the detected information and risks of the server.

Figure 1-15 Viewing the detection result



Type	Quantity
Account Information	4
Open Ports	93
Processes	100
Installed Software	157
Auto-startup	223
Web applications	0
Web services	1
Web frameworks	0
Websites	0
Middleware	210
Databases	0
Kernel Module	0

□	Local Port	Listening IP address	Status	PID	Program File
□	445	[redacted]	--	4	C:\Windows\System32\ntoskrnl.exe
□	3389	[redacted]	--	1448	C:\windows\System32\svchost.exe
□	49666	[redacted]	--	1700	C:\windows\system32\svchost.exe
□	49666	[redacted]	--	1700	C:\windows\system32\svchost.exe
□	49669	[redacted]	--	2964	C:\windows\system32\svchost.exe
□	49665	[redacted]	--	852	C:\Windows\System32\wininit.exe
□	65501	[redacted]	--	19296	C:\elite\IdpLocalService\jre\bin\idplite...

Follow-up Procedure

You can manually configure check items. Configurable items vary according to the edition you enabled.

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

Figure 1-16 Manual check items

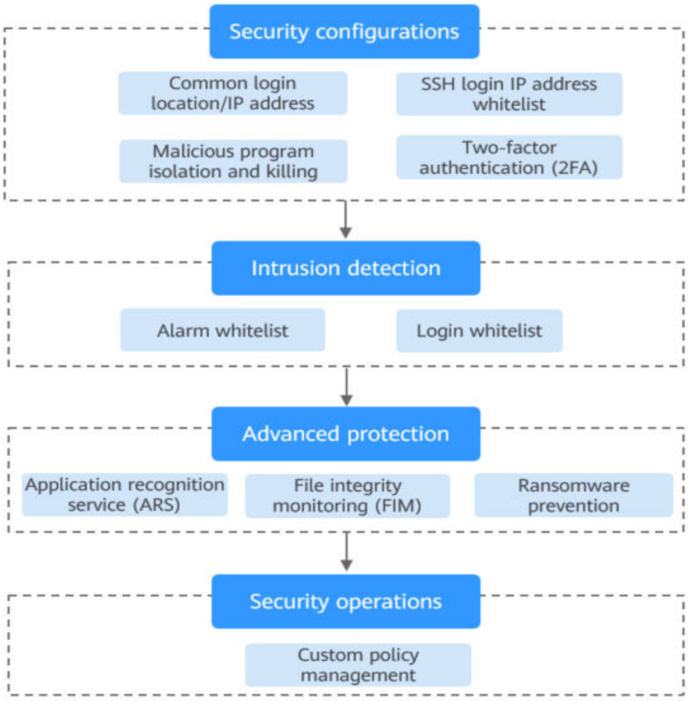

Security configurations
Common login location/IP address
SSH login IP address whitelist
Malicious program isolation and killing
Two-factor authentication (2FA)
Intrusion detection
Alarm whitelist
Login whitelist
Advanced protection
Application recognition service (ARS)
File integrity monitoring (FIM)
Ransomware prevention
Security operations
Custom policy management

Table 1-6 Manual check items

Function	Check Item	Reference
Installation and configuration	● Common login location/IP address ● SSH login IP address whitelist ● Isolate and kill malicious programs	**Common Security Configuration**
Intrusion detection	● Alarm whitelist ● Login Whitelist configuration	**Intrusion Detection**
Proactive defense	● Application protection ● Ransomware prevention ● File integrity monitoring (FIM)	**Prevention**
Security operations	● Policy management	**Security Operations**
Security report	● Subscribe to security reports	**Subscribing to a Security Report**

Related Operations

Disabling HSS

On the **Servers** tab of the **Servers & Quotas** 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 attacks.
- 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 **Asset Management** > **Servers & Quota**, and click the **Quotas** tab. Click **Unbind** in the **Operation** column. The usage status of the unbound quota will change from **In use** to **Idle**. HSS will automatically disable protection for the server unbound from the quota.

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

1.4.2 Enabling Web Tamper Protection

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.

How WTP Prevents Web Page Tampering

Table 1-7 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	Provides runtime application self-protection (RASP) for Tomcat applications in the following ways: 1. Malicious behavior filtering based on RASP The Huawei-unique runtime application self-protection (RASP) detects application program behaviors, preventing attackers from tampering with web pages through application programs. 2. Network disk file access control WTP implements fine-grained management to control permissions for adding, modifying, and querying file content in network disks, preventing tampering without affecting website content release.

Prerequisites

- Choose **Prevention** > **Web Tamper Protection**. Click the **Servers** tab. The **Protection Status** of the server is **Unprotected**.
- Choose **Asset Management** > **Servers & Quota**. The **Agent Status** of a server is **Online**, and the **Protection Status** of the server is **Unprotected**.

Setting Protected Directories

You can set:

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

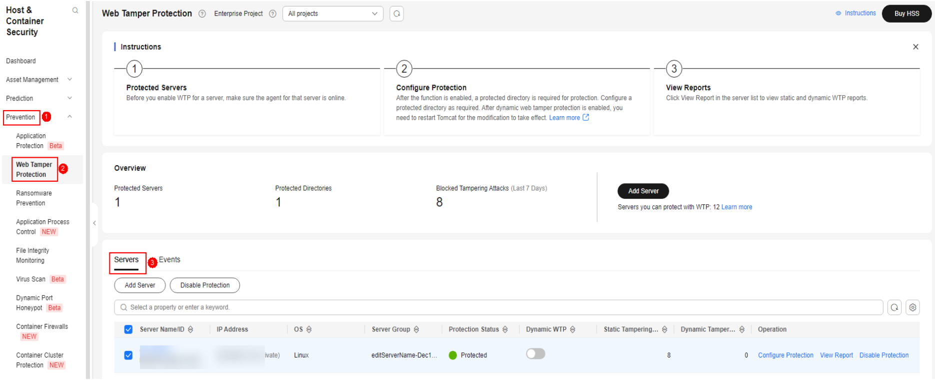
Enabling WTP

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

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **HSS** to go to the HSS management console.

Step 3 In the navigation pane, choose **Prevention** > **Web Tamper Protection**. On the **Web Tamper Protection** page, click **Add Server**.

Figure 1-17 Adding a protected server



Instructions

1 Protected Servers
Before you enable WTP for a server, make sure the agent for that server is online.

2 Configure Protection
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

3 View Reports
Click View Report in the server list to view static and dynamic WTP reports.

Overview

Protected Servers	Protected Directories	Blocked Tampering Attacks (Last 7 Days)
1	1	8

Add Server
Servers you can protect with WTP: 12 Learn more

☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑	[redacted]	[redacted]ivate)	Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 4 On the **Add Server** page, click the **Available servers** tab. Select the target server, select a quota from the drop-down list or retain the default value, and click **Add and Enable Protection**.

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

The premium edition will be enabled when you enable WTP.

- Choose **Prevention** > **Web Tamper Protection**. If the **Protection Status** of the server is **Protected**, WTP has been enabled.
- Choose **Asset Management** > **Servers & Quota** and click the **Servers** tab. 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

NOTICE

- To enable WTP protection for a server, you can also choose **Asset Management** > **Servers & Quota**, click the **Quotas** tab, and click **Bind Server**.
- A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- If the version of the agent installed on the Linux server is 3.2.10 or later or the version of the agent installed on the Windows server is 4.0.22 or later, ransomware prevention is automatically enabled with the WTP edition. Deploy bait files on servers and automatically isolate suspicious encryption processes (there is a low probability that processes are incorrectly isolated). You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Enabling Ransomware Backup**.
- 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.

Related Operations

Disabling WTP

Choose **Prevention** > **Web Tamper Protection** and click the **Servers** tab. Click **Disable Protection** 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 prevent 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

Choose **Asset Management** > **Servers & Quota**, and click the **Quotas** tab. Click **Unbind** in the **Operation** column. The usage status of the unbound quota will change from **In use** 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.

1.4.3 Enabling Container Protection

Before enabling protection for a container node, you need to allocate quota to a specified node. If the protection is disabled or the node is deleted, the quota can be allocated to other nodes.

Check Frequency

HSS performs a full check in the early morning every day.

If you enable server protection before the check interval, you can view check results only after the check at 00:00 of the next day is complete.

Constraints

Currently, HSS can only protect Docker and Containerd containers.

Prerequisites

- The **Agent Status** of a server is **Online**. To check the status, choose **Asset Management** > **Containers & Quota**.
- You have created nodes on CCE.
- The **Protection Status** of the node is **Unprotected**.

Procedure

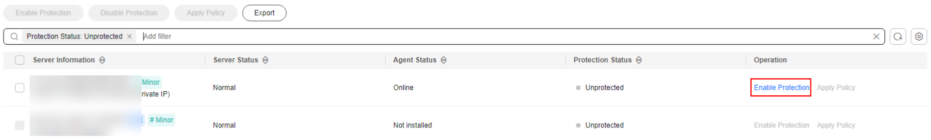
Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 4 In the **Operation** column of the node list, click **Enable Protection**.

Figure 1-18 Enabling container protection



Protection Status: Unprotected | Add filter

Server Information	Server Status	Agent Status	Protection Status	Operation
Minor rivate IP)	Normal	Online	Unprotected	Enable Protection Apply Policy
# Minor	Normal	Not installed	Unprotected	Enable Protection Apply Policy

Step 5 You can buy quota in pay-per-use or yearly/monthly mode.

- **Yearly/Monthly**

  In the displayed dialog box, select **Yearly/Monthly**, read the *Container Guard Service Disclaimer*, and select **I have read and agreed to Container Guard Service Disclaimer**.

  The quotas can be allocated in the following ways:

  - Select **Random quota** to let the system allocate the quota with the longest remaining validity to the server.
  - Select a quota to allocate.
- **Pay-per-use**

  In the displayed dialog box, select **Pay-per-use**, read the *Container Guard Service Disclaimer*, and select **I have read and agreed to Container Guard Service Disclaimer**.

Step 6 In the displayed dialog box, read the *Container Guard Service Disclaimer*, and select **I have read and agreed to the Container Guard Service Disclaimer**.

Step 7 Click **OK**. If the **Protection Status** of the server changes to **Protected**, protection has been enabled.

NOTE

A container security quota protects one cluster node.

- A container security quota protects one cluster node.
- If the version of the agent installed on the Linux server is 3.2.10 or later or the version of the agent installed on the Windows server is 4.0.22 or later, ransomware prevention is automatically enabled with the container edition. Deploy bait files on servers and automatically isolate suspicious encryption processes (there is a low probability that processes are incorrectly isolated). You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Enabling Ransomware Backup**.

----End

Related Operations

Disabling protection for a node

Choose **Asset Management** > **Containers & Quota**, click the **Container Nodes** tab, and click **Nodes**. In the **Operation** column, click **Disable Protection**.

If protection is disabled, the quota status will change from occupied to idle. You can allocate the idle quota to another node or unsubscribe unnecessary quota to avoid quota waste.

NOTICE

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

1.5 Enabling Alarm Notifications

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.

- 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 blocked. If you have enabled notifications but not received any, check whether they have been blocked as spasms.
- The Simple Message Notification (SMN) service is a paid service. For details about the price, see **Product Pricing Details**.

Enabling 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** > **HSS**.

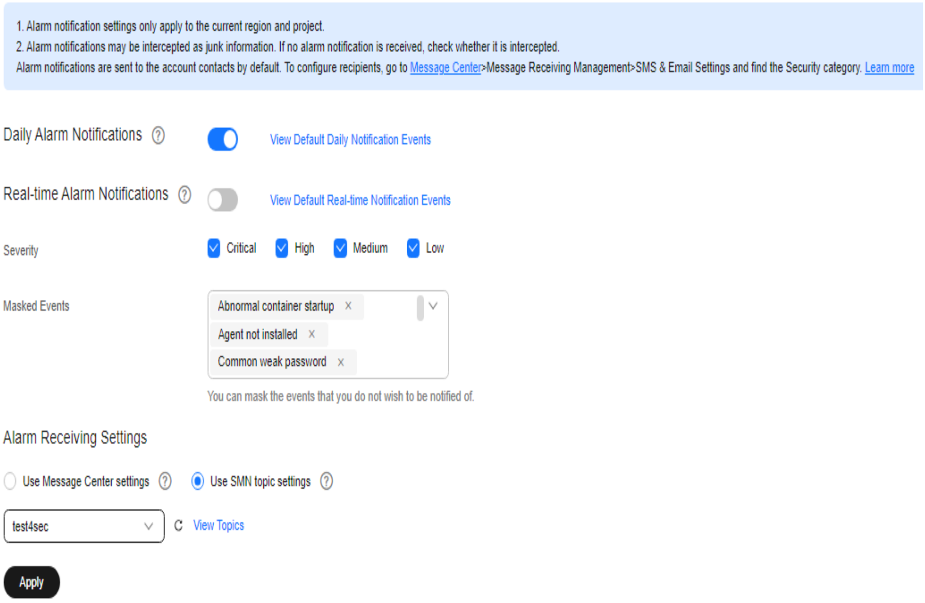
Step 3 In the navigation pane, choose **Installation & Configuration**, and click **Alarm Notifications**. **Table 1-8** describes the parameters.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to configure alarm notifications.

- If you select a single enterprise project, the alarm notification information takes effect only in the corresponding enterprise project.
- If you select **All projects**, the alarm notification information takes effect in all enterprise projects.

Figure 1-19 Alarm configurations



1. Alarm notification settings only apply to the current region and project.
2. Alarm notifications may be intercepted as junk information. If no alarm notification is received, check whether it is intercepted.
Alarm notifications are sent to the account contacts by default. To configure recipients, go to Message Center>Message Receiving Management>SMS & Email Settings and find the Security category. Learn more

Daily Alarm Notifications: on — View Default Daily Notification Events

Real-time Alarm Notifications: off — View Default Real-time Notification Events

Severity: ☑ Critical ☑ High ☑ Medium ☑ Low

Masked Events: Abnormal container startup ×, Agent not installed ×, Common weak password ×

You can mask the events that you do not wish to be notified of.

Alarm Receiving Settings

○ Use Message Center settings ● Use SMN topic settings

test4sec — View Topics

Apply

Table 1-8 Alarm configurations

Notification Item	Description	Suggestion
Daily alarm notification	HSS 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, depending on which one you chose. To view notification items, click **View Default Daily Notification Events**.	● 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**.
Real-time alarm notification	When an attacker intrudes a server, alarms are sent to the recipients you set in the Message Center or SMN, depending on which one you chose. To view notification items, click **View Default Real-time Notification Events**.	● 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**.
Severity	Select the severities of alarms that you want to be notified of.	All
Masked Events	Select the events that you do not wish to be notified of. Select events to be masked from the drop-down list box.	Determine the events to be masked based on the description in **Alarm Notifications**.

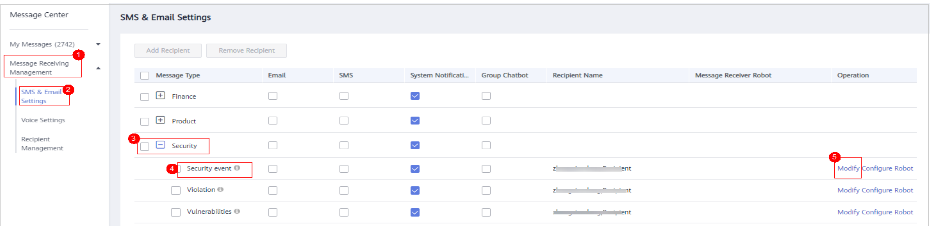
Step 4 Select the alarm notification mode.

- **Use Message Center settings**

  By default, alarm notifications are sent to the recipients specified in your message center. You can log in to your account to check your recipient settings.

To configure recipients, choose **Message Receive Management** > **SMS & Email Settings**. In the **Security** area, click **Modify** in the row where **Security event** resides.

Figure 1-20 Editing message recipients



Message Type	Email	SMS	System Notificati...	Group Chatbot	Recipient Name	Message Receiver Robot	Operation
□ ⊞ Finance	□	□	☑	□			
□ ⊞ Product	□	□	☑	□			
□ ⊟ Security	□	□	☑	□			
□ Security event	□	□	☑	□	[redacted]		Modify Configure Robot
□ Violation	□	□	☑	□	[redacted]		Modify Configure Robot
□ Vulnerabilities	□	□	☑	□	[redacted]		Modify Configure Robot

- **Use 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. Create a topic. For details, see **Creating 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

Alarm Notifications

- **Daily Alarm Notifications**

  The service 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.

Table 1-9 Daily alarm notification

Type	Item	Description
Assets	Dangerous ports	Check for high-risk open ports and unnecessary ports.

Type	Item	Description
	Agent not installed	Check for servers with no HSS agent installed, and remind you to install the agent on these servers in a timely manner.
Vulnerabilities	Critical vulnerabilities	Detect critical vulnerabilities and fix them in a timely manner.
Unsafe settings	Unsafe configurations	Detect unsafe settings of key applications that will probably be exploited by hackers to intrude servers.
	Common weak passwords	Detect weak passwords in MySQL, FTP, and system accounts.
Intrusions	Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojan, mining software, worms, and viruses.
	Rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.
	Ransomware	Check for ransomware in media such as web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.
	Web shells	Check whether the files (often PHP and JSP files) detected by HSS 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.
	Reverse shells	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.
	Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms.

Type	Item	Description
	Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms.
	MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms.
	File privilege escalations	Check the file privilege escalations in your system.
	Process privilege escalations	The following process privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities
	Important file changes	Receive alarms when critical system files are modified.
	File/ Directory change	System files and directories are monitored. If a file or directory is modified, an alarm is generated, indicating that the file or directory may be tampered with.
	Abnormal process behaviors	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
	High-risk command executions	Check executed commands in real time and generate alarms if high-risk commands are detected.
	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.

Type	Item	Description
	Suspicious crontab tasks	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.
	Container image blocking	If a container contains insecure images specified in suspicious image behaviors, an alarm will be generated and the insecure images will be blocked before a container is started in Docker.
	Brute-force attacks	Check for brute-force attack attempts and successful brute-force attacks. ● Detect password cracking attacks on accounts and block attacking IP addresses to prevent server intrusion. ● Trigger an alarm if a user logs in to the server by a brute-force attack.
	Abnormal logins	Check and handle remote logins. If a user's login location is not any common login location, an alarm will be triggered.
	Invalid accounts	Scan accounts on servers and list suspicious accounts in a timely manner.
	Vulnerability escapes	The service reports an alarm if it detects container process behavior that matches the behavior of known vulnerabilities (such as Dirty COW, brute-force attack, runC, and shocker).
	File escapes	The service reports an alarm if it detects that a container process accesses a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms.
	Abnormal container processes	Container services are usually simple. If you are sure that only specific processes run in a container, you can add the processes to the whitelist of a policy, and associate the policy with the container. The service reports an alarm if it detects that a process not in the whitelist is running in the container.

Type	Item	Description
	Abnormal container startups	Check for unsafe parameter settings used during container startup. Certain startup parameters specify container permissions. If their settings are inappropriate, they may be exploited by attackers to intrude containers.
	High-risk system calls	Users can run tasks in kernels by Linux system calls. The service reports an alarm if it detects a high-risk call, such as **open_by_handle_at**, **ptrace**, **setns**, and **reboot**.
	Sensitive file access	Detect suspicious access behaviors (such as privilege escalation and persistence) on important files.
	Web page tampering prevention for Windows servers	Protect the static web page files on your Windows website servers from malicious modification.
	Web page tampering prevention for Linux servers	Protect the static web page files on your Linux website servers from malicious modification.
	Dynamic WTP	Protect the static web page files on your Windows and Linux website servers from malicious modification.
	Application protection	Protect running applications. You simply need to add probes to applications, without having to modify application files. Currently, only Linux servers are supported, and only Java applications can be connected.
	Virus scan	Generates alarms for detected virus-infected files.

- **Real-Time Alarm Notifications**

  When an event occurs, an alarm notification is immediately sent.

Table 1-10 Real-time alarm notification

Notification Item	Item	Description
Intrusions	Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojans, mining software, worms, and viruses.
	Rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.
	Ransomware	Check for ransomware in media such as web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.
	Web shells	Check whether the files (often PHP and JSP files) detected by HSS 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.
	Reverse shells	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.
	Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms.
	Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms.
	MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms.
	File privilege escalations	Check the file privilege escalations in your system.

Notification Item	Item	Description
	Process privilege escalations	The following process privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities
	Critical file changes	Receive alarms when critical system files are modified.
	File/ Directory changes	System files and directories are monitored. When a file or directory is modified, an alarm is generated, indicating that the file or directory may be tampered with.
	Abnormal process behavior detection	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
	Detecting High-Risk Command Execution	Check executed commands in real time and generate alarms if high-risk commands are detected.
	Abnormal shell detection	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.
	Suspicious crontab tasks	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.
	Container image blocking	If a container contains insecure images specified in suspicious image behaviors, an alarm will be generated and the insecure images will be blocked before a container is started in Docker.

Notification Item	Item	Description
	Exception Stat	Check and handle remote logins. If a user's login location is not any common login location you set, an alarm will be triggered.
	Invalid account	Scan accounts on servers and list suspicious accounts in a timely manner.
	Vulnerability escapes	The service reports an alarm if it detects container process behavior that matches the behavior of known vulnerabilities (such as Dirty COW, brute-force attack, runC, and shocker).
	File escapes	The service reports an alarm if it detects that a container process accesses a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms.
	Abnormal container processes	Container services are usually simple. If you are sure that only specific processes run in a container, you can add the processes to the whitelist of a policy, and associate the policy with the container. The service reports an alarm if it detects that a process not in the whitelist is running in the container.
	Abnormal container startups	Check for unsafe parameter settings used during container startup. Certain startup parameters specify container permissions. If their settings are inappropriate, they may be exploited by attackers to intrude containers.
	High-risk system calls	Users can run tasks in kernels by Linux system calls. The service reports an alarm if it detects a high-risk call, such as **open_by_handle_at**, **ptrace**, **setns**, and **reboot**.
	Sensitive file access	Detect suspicious access behaviors (such as privilege escalation and persistence) on important files.
	Web page tampering prevention for Windows servers	Protect the static web page files on your Windows website servers from malicious modification.

Notification Item	Item	Description
	Web page tampering prevention for Linux servers	Protect the static web page files on your Linux website servers from malicious modification.
	Dynamic WTP	Protect the static web page files on your Windows and Linux website servers from malicious modification.
	Application protection	Protect running applications. You simply need to add probes to applications, without having to modify application files. Currently, only Linux servers are supported, and only Java applications can be connected.
	Brute-force attacks	Check for brute-force attack attempts and successful brute-force attacks. ● Detect password cracking attacks on accounts and block attacking IP addresses to prevent server intrusion. ● Trigger an alarm if a user logs in to the server by a brute-force attack.
	Auto Blocking	Notify users of successful automatic isolation and killing of malicious programs, automatic blocking of ransomware, and automatic blocking of WTP.
Login	Success login	Notifications are sent to accounts that have successfully logged in.

1.6 Common Security Configuration

1.6.1 Configuring Server Login Protection

You can configure common login locations, common login IP addresses, and an SSH login IP address 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** > **HSS**.

----End

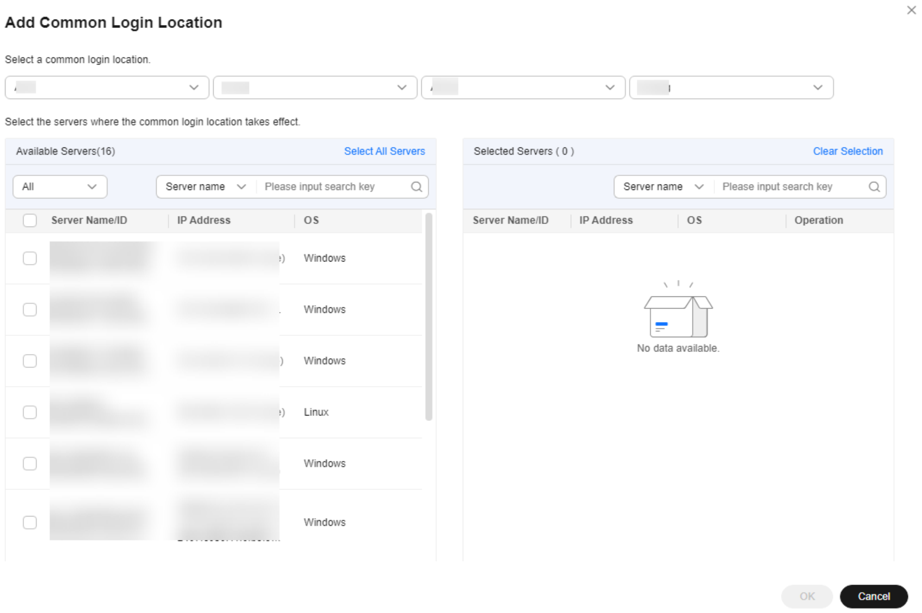
Configuring Common Login Locations

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 Choose **Installation & Configuration** and click the **Security Configuration** tab. Click **Common Login Locations** and click **Add Common Login Location**.

Step 2 In the dialog box that is displayed, select a geographical location and select servers. Confirm the information and click **OK**.

Figure 1-21 Configuring common login locations



Add Common Login Location

Select a common login location.

Select the servers where the common login location takes effect.

Available Servers(16)

Server Name/ID	IP Address	OS
		Windows
		Windows
		Windows
		Linux
		Windows
		Windows

Selected Servers (0)

Server Name/ID	IP Address	OS	Operation

No data available.

Step 3 Return to the **Security Configuration** tab of the **Installation & Configuration** page. Check whether the added locations are displayed on the **Common Login Locations** subtab.

NOTE

HSS has a learning process for remote login alarms. Therefore, after common login locations are added, the first three login locations are regarded as common login locations, and alarms are generated only for the fourth and subsequent non-common login locations.

----End

Configuring Common Login IP Addresses

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

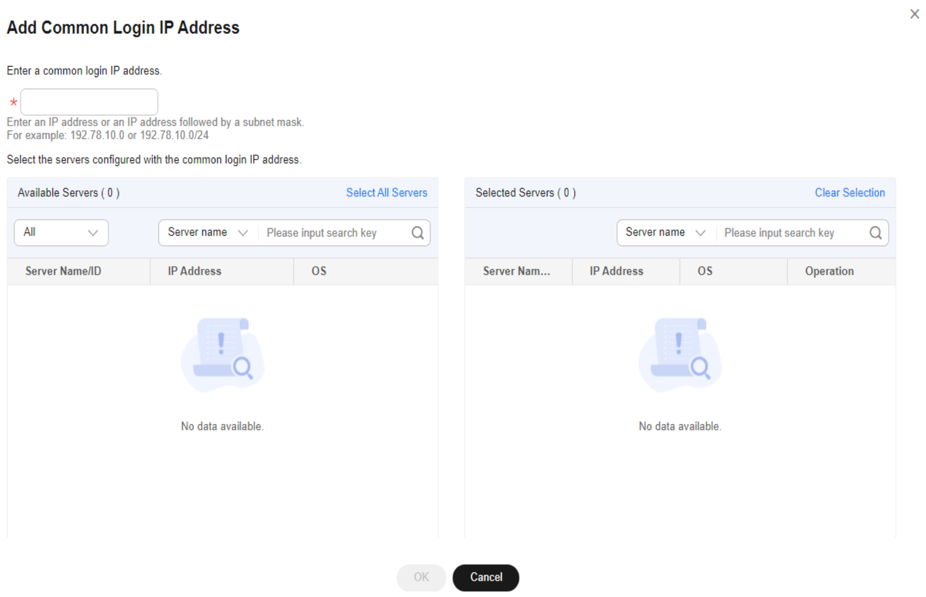
Step 1 Choose **Installation & Configuration** and click the **Security Configuration** tab. Click **Common Login IP Addresses** and click **Add Common Login IP Address**.

Step 2 In the dialog box that is displayed, enter an IP address and select servers. Confirm the information and click **OK**.

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.
- Only one IP address can be added at a time. To add multiple IP addresses, repeat the operations until all IP addresses are added. Up to 20 IP addresses can be added.

Figure 1-22 Entering a common login IP address



Add Common Login IP Address

Enter a common login IP address.

*

Enter an IP address or an IP address followed by a subnet mask.
For example: 192.78.10.0 or 192.78.10.0/24

Select the servers configured with the common login IP address.

Step 3 Return to the **Security Configuration** tab of the **Installation & Configuration** page. Check whether the added locations are displayed on the **Common Login IP Addresses** subtab.

----End

Configuring an SSH Login IP Address Whitelist

The SSH login whitelist controls SSH access to servers to prevent account cracking.

NOTE

- An account can have up to 10 SSH login IP addresses in the whitelist.
- 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.

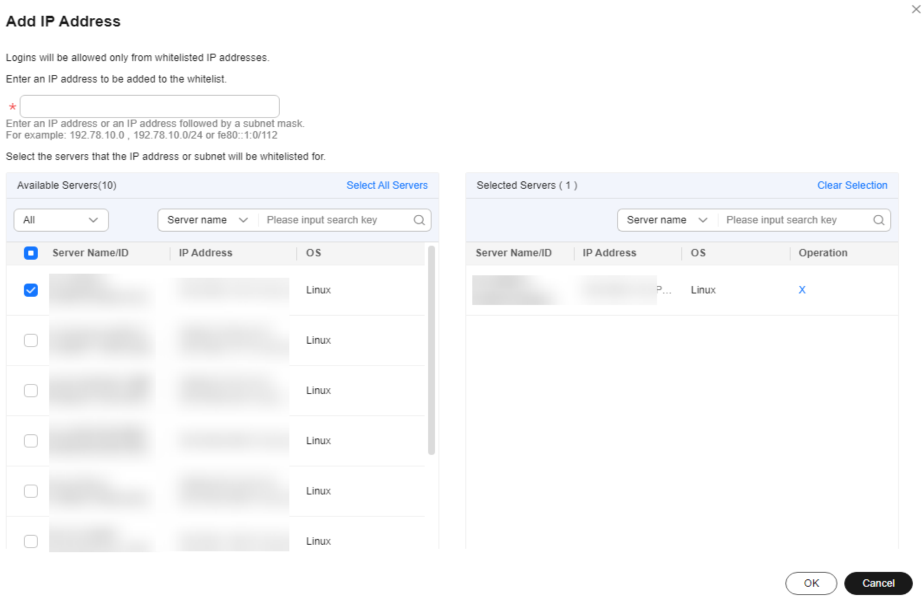
Step 1 Choose **Installation & Configuration** and click the **Security Configuration** tab. Click **SSH IP Whitelist** and click **Add IP Address**.

Step 2 In the dialog box that is displayed, enter an IP address and select servers. Confirm the information and click **OK**.

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.
- Only one IP address can be added at a time. To add multiple IP addresses, repeat the operations until all IP addresses are added.

Figure 1-23 Entering an IP address



Add IP Address

Logins will be allowed only from whitelisted IP addresses.

Enter an IP address to be added to the whitelist.

*

Enter an IP address or an IP address followed by a subnet mask.
For example: 192.78.10.0 , 192.78.10.0/24 or fe80::1:0/112

Select the servers that the IP address or subnet will be whitelisted for.

Available Servers(10) — Select All Servers

All | Server name | Please input search key

■	Server Name/ID	IP Address	OS
☑	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux

Selected Servers (1) — Clear Selection

Server name | Please input search key

Server Name/ID	IP Address	OS	Operation
[redacted]	[redacted]P...	Linux	X

Step 3 Return to the **Security Configuration** tab of the **Installation & Configuration** page. Check whether the added locations are displayed on the **Common Login IP Addresses** subtab.

----End

1.6.2 Isolating and Killing Malicious Programs

HSS automatically isolates and kills identified malicious programs, such as web shells, Trojans, and worms, removing security risks.

Programs are isolated and killed based on their confidence ratings. A high rating indicates a high probability that the detected program is a malicious program. To avoid mistakenly stopping trustworthy programs and affecting services, only the suspicious programs with a confidence rating of 95 or higher are automatically isolated and killed. You can manually isolate and kill programs with lower ratings. For details, see **Handling Server Alarms**.

NOTE

To check the confidence rating of a suspicious program, choose **Detection** > **Alarms** on the HSS console, and click **Server Alarms**. Click a malicious program alarm name to view details.

Procedure

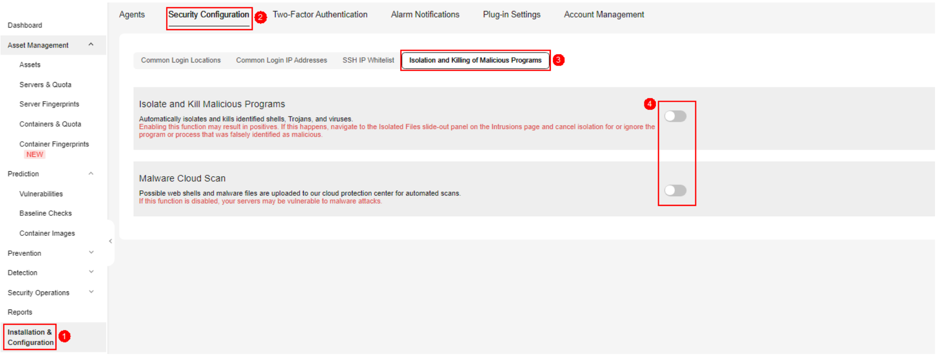
Step 1 Log in to the management console.

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

Step 3 Choose **Installation & Configuration** and click the **Security Configuration** tab. Click the **Isolation and Killing of Malicious Programs** tab and enable **Isolate and Kill Malicious Programs** and **Malware Cloud Scan**.

> NOTE
>
> After the cloud scan function is enabled, all HSS servers will be scanned. Some HSS quota editions can support only limited scanning capabilities. Therefore, you are advised to enable the enterprise edition or higher to enjoy all capabilities of the isolation and killing function.

Figure 1-24 Enabling isolation and killing



Isolate and Kill Malicious Programs

Automatically isolates and kills identified shells, Trojans, and viruses.
Enabling this function may result in positives. If this happens, navigate to the Isolated Files slide-out panel on the Intrusions page and cancel isolation for or ignore the program or process that was falsely identified as malicious.

Malware Cloud Scan

Possible web shells and malware files are uploaded to our cloud protection center for automated scans.
If this function is disabled, your servers may be vulnerable to malware attacks.

Step 4 In the confirmation dialog box, click **OK** to enable the isolation and killing of malicious programs and malware cloud scan.

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 **Viewing Server Alarms**.

> 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**.

----End

1.6.3 Enabling 2FA

Two-factor authentication (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

- You have created a message topic whose protocol is SMS or email.
- Server protection has been enabled.
- To enable 2FA, 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.

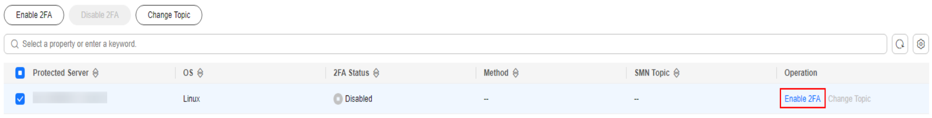
Constraints and Limitations

- If 2FA is enabled, it can be used only in following scenarios:
  - Linux: The SSH password is used to log in to an ECS, and the OpenSSH version is earlier than 8.
  - Windows: The RDP file is used to log in to a Windows ECS.
- When two-factor authentication is enabled for Windows ECSs, the **User must change password at next logon** function is not allowed. To use this function, disable two-factor authentication.

Procedures

Step 1 On the **Two-Factor Authentication** tab, select servers and click Enable **2FA**. Alternatively, click **Enable** in the **Operation** column.

Figure 1-25 Enable 2FA.



☐ Protected Server	OS	2FA Status	Method	SMN Topic	Operation
☑ [redacted]	Linux	Disabled	--	--	Enable 2FA Change Topic

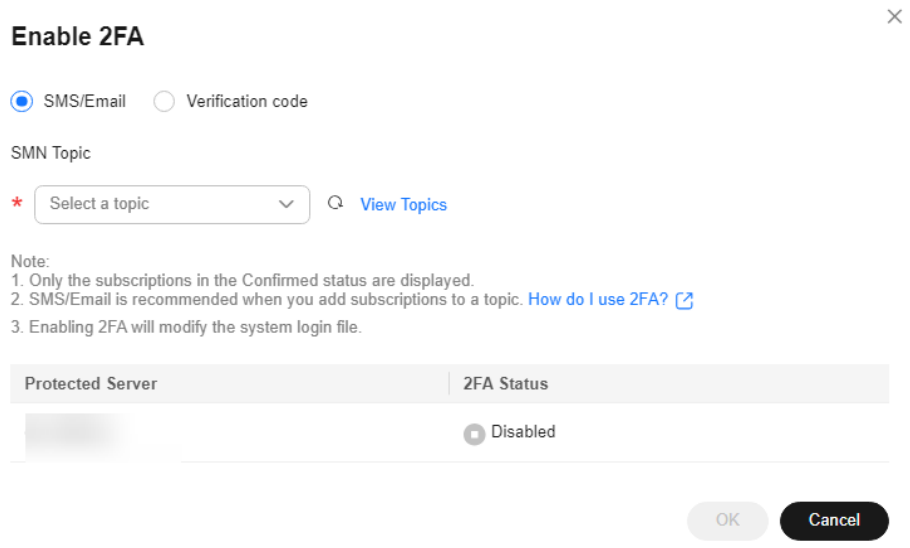
Step 2 In the displayed **Enable 2FA** dialog box, select an authentication mode.

- **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 1-26 SMS/Email verification



Enable 2FA

● SMS/Email ○ Verification code

SMN Topic

* Select a topic View Topics

Note:
1. Only the subscriptions in the Confirmed status are displayed.
2. SMS/Email is recommended when you add subscriptions to a topic. How do I use 2FA?
3. Enabling 2FA will modify the system login file.

Protected Server	2FA Status
	Disabled

- **Verification code**

  Use the verification code you receive in real time for verification.

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

2 Dashboard

On the HSS dashboard, you can check the security score, risks, and protection overview of all your assets in real time, including servers and containers.

Viewing the Dashboard Page

Step 1 Log in to the management console.

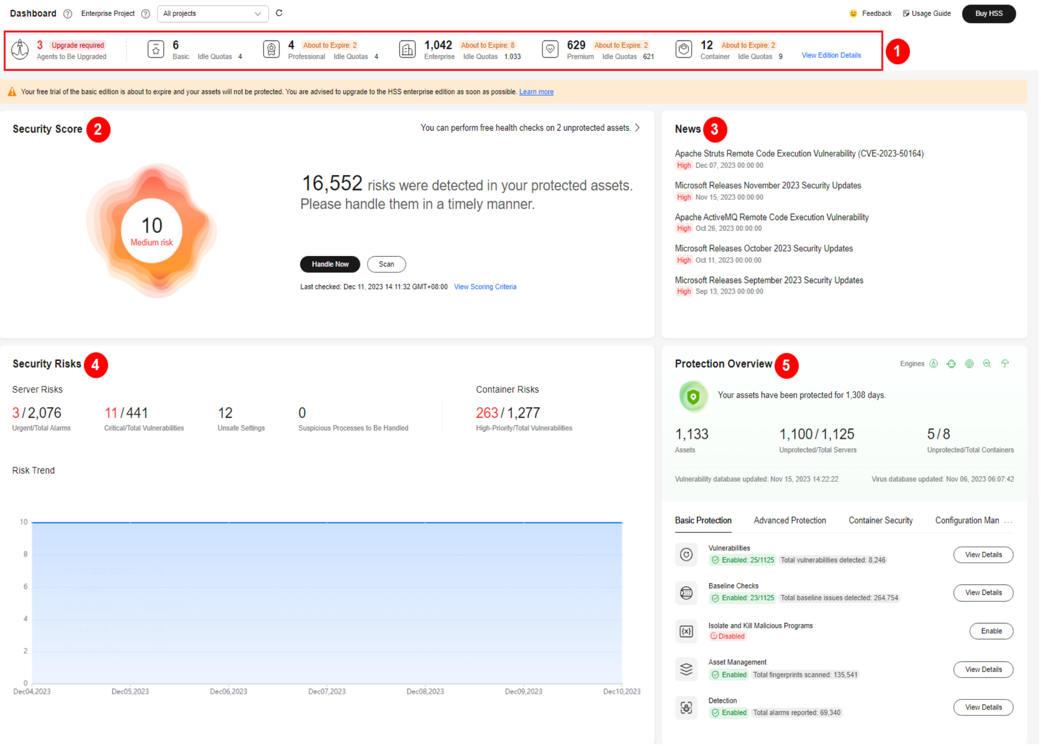
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 In the navigation pane, choose **Dashboard** and check the security overview. For more information, see **Table 2-1**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Figure 2-1 Dashboard



Your free trial of the basic edition is about to expire and your assets will not be protected. You are advised to upgrade to the HSS enterprise edition as soon as possible. Learn more

You can perform free health checks on 2 unprotected assets.

16,552 risks were detected in your protected assets. Please handle them in a timely manner.

Last checked: Dec 11, 2023 14:11:32 GMT+08:00

Apache Struts Remote Code Execution Vulnerability (CVE-2023-50164)
High Dec 07, 2023 00:00:00

Microsoft Releases November 2023 Security Updates
High Nov 15, 2023 00:00:00

Apache ActiveMQ Remote Code Execution Vulnerability
High Oct 26, 2023 00:00:00

Microsoft Releases October 2023 Security Updates
High Oct 11, 2023 00:00:00

Microsoft Releases September 2023 Security Updates
High Sep 13, 2023 00:00:00

Your assets have been protected for 1,308 days.

Vulnerability database updated: Nov 15, 2023 14:22:22

Virus database updated: Nov 06, 2023 06:07:42

Total vulnerabilities detected: 8,246

Total baseline issues detected: 264,754

Total fingerprints scanned: 135,541

Total alarms reported: 69,340

Table 2-1 Dashboard components

Component	Description
Quotas and agents to be upgraded (component 1 in **Dashboard**)	HSS edition quotas and their usage, and the number of agents to be upgraded. ● Click the number of quotas to go to quota list. ● Click the number of agents to be upgraded to go to the agent list and upgrade agents. **NOTE** HSS will be continuously upgraded to provide new features and fix bugs. To enjoy better HSS features, upgrade the agent to the latest version in a timely manner. For details, see **Upgrading the agent**.

Component	Description
Secure score (component 2 in **Dashboard**)	The security score is in the range 0 to 100. The default score for risk-free assets is 100. Points are deducted based on baseline risks, vulnerability risks, intrusion risks, and asset risks. A low score indicates high security risks in assets. To ensure the security of your assets, you are advised to handle security risks in a timely manner and improve the security score. 1. In the **Security Score** area, click **Handle Now**. 2. In the **Handle Now** dialog box, view the deduction items and click ⌄ to expand the details. 3. Click **Handle** on the right of deduction items to go to the corresponding risk list. You can rectify the fault based on the risk details and handling suggestions. For details about the score deduction items and how to increase the score, see **Security Scores Criteria and Methods for Improving Scores**. 4. After the risk is fixed, click **Scan** to update the score.
News (component 3 in **Dashboard**)	Latest vulnerability information.

Component	Description
Security risk (component 4 in **Dashboard**)	Security risks detected by HSS in your assets. ● **Server Risks** – **Urgent/Total Alarms**: Number of alarms that need to be handled immediately and the total number of alarms. You can click the number of urgent alarms to go to the **Alarms** page and handle alarms. For details, see **Handling Server Alarms**. – Critical/Total Vulnerabilities: Number of critical vulnerabilities and the total number of vulnerabilities. You can click the number of critical vulnerabilities to go to the **Vulnerabilities** page and handle vulnerabilities. For details, see **Handling Vulnerabilities**. – **Unsafe Settings**: Number of baseline risks to be handled. You can click the number to go to the **Baseline Checks** page and fix baseline risks. For details, see **Viewing and Processing Baseline Check Results**. – **Suspicious Processes to Be Handled**: Total number of suspicious processes to be handled. You can click the number of suspicious processes to be handled to go to the **Application Process Control** page and handle suspicious processes. For details, see **Checking and Handling Suspicious Processes**. ● **Container Risks** **High-Priority/Total Vulnerabilities**: Number of high-risk vulnerabilities and the total number of vulnerabilities. You can click the number of high-priority vulnerabilities to go to the **Image Vulnerabilities** tab and check vulnerability fixing suggestions. For details, see **SWR Image Repository Vulnerabilities**. ● **Risk Trend** Asset risk trend in the last seven days.

Component	Description
Protection overview (component 5 in **Dashboard**)	Asset protection overview. ● **Assets**: Total number of assets in the current region. You can click the total number of assets to go to the **Assets** page to view asset distribution and protection status. ● **Unprotected/Total Servers**: Number of unprotected servers and the total number of servers. You can click the number of unprotected servers to go to the **Servers & Quota** page to view servers and enable protection. For details, see **Enabling Protection**. ● **Unprotected/Total Containers**: Number of unprotected containers and the total number of containers. You can click the number of unprotected containers to go to the **Containers & Quota** page to view containers and enable protection. For details, see **Enabling Container Protection**. ● Vulnerability or virus database update time: The latest update time of the vulnerability or virus database. ● Security feature status: The number of servers protected by each feature and the number of items detected by each feature. You can click **View Details** to go to corresponding feature page.
Best Practices	HSS best practices. Click a title to view details.
FAQ	HSS best FAQ. Click a title to view details.
Related Services	Security services related to HSS. Click a service name to go to its console.

----End

Security Scores Criteria and Methods for Improving Scores

The security score for risk-free assets is 100. A low score indicates high security risks in assets. HSS calculates your security score based on detected security items (vulnerabilities, compliance, intrusions, assets, and images) and unprotected assets. Scores are deducted every time a risk is detected in a category until all scores in that category are deducted. The full score of each category is as follows:

- No vulnerabilities detected: 20. For details about the score deduction criteria and improvement methods, see **Table 2-2**.
- No compliance risks detected: 20. For details about the score deduction criteria and improvement methods, see **Table 2-3**.

- No intrusion risks detected: 30. For details about the score deduction criteria and improvement methods, see **Table 2-4**.
- No asset risks detected: 10. For details about the score deduction criteria and improvement methods, see **Table 2-5**.
- No image risks detected: 10. For details about the score deduction criteria and improvement methods, see **Table 2-6**.
- No unprotected assets detected: 10. For details about the score deduction criteria and improvement methods, see **Table 2-7**.

Table 2-2 Vulnerability risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unhandled vulnerabilities	Unhandled critical vulnerabilities	All	10	√	Fix vulnerabilities based on the suggestions provided, scan for vulnerabilities again, and update the score. ● For details about how to fix vulnerabilities, see **Handling Vulnerabilities**. ● For details about how to scan for vulnerabilities, see **Vulnerability Scan**.
	Unhandled high-risk vulnerabilities	All	3	√	
	Unhandled medium-risk vulnerabilities	All	1	√	
	Unhandled low-risk vulnerabilities	All	0.1	√	

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
No vulnerability scan	No vulnerability scans were performed in the past month.	All	15	×	● The basic edition HSS does not provide vulnerability scan. To use this feature, upgrade HSS to the enterprise or premium edition. For details, see **Upgrading Protection Quotas**. ● In HSS professional, enterprise, premium, and WTP editions, you are advised to perform vulnerability scans. For details, see **Scanning Vulnerabilities**.

Table 2-3 Compliance risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unhandled non-compliance items	Unhandled high-risk non-compliance items	All	10	√	Rectify non-compliance items, perform a baseline check again, and update the score. ● For details about how to fix baseline risks, see **Viewing and Processing Baseline Check Results**. ● For details about how to perform baseline check, see **Performing Baseline Check**.
	Unhandled medium-risk non-compliance items	All	3	√	

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
	Unhandled low-risk non-compliance items	All	1	√	
Weak passwords	Weak passwords	All	10	√	Use strong passwords. For details, see **How Do I Set a Secure Password?**
Weak password check not enabled	Weak password check policy not enabled	All	10	×	Enable the **Weak Password Detection** policy to check for weak passwords on servers. For details, see **Overview**.
Baseline check not performed	No baseline checks were performed in the past month.	All	10	×	● The HSS basic and professional editions do not provide baseline check. To use this feature, you are advised to upgrade HSS to the enterprise or premium edition. For details, see **Upgrading Protection Quotas**. ● In HSS professional, enterprise, premium, and WTP editions, you are advised to perform baseline checks. For details, see **Viewing and Editing a Policy**.

Table 2-4 Intrusion risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unhandled alarms	Critical alarms not fixed	All	10	√	Handle alarms based on the suggestions provided. After alarms are handled, HSS will automatically update the score. For details, see **Handling Server Alarms** and **Handling Container Alarms**.
	Unhandled high-risk alarms	All	3	√	
	Unhandled medium-risk alarms	All	1	√	
	Unhandled low-risk alarms	All	0.1	√	

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Protection not enabled	No security policies enabled	All	30	×	In the HSS professional, enterprise, premium, WTP, and container editions, you need to enable protection policies. For details, see **Overview**. The intrusion detection policies that need to be enabled for each edition are as follows: ● Professional/Enterprise edition – Linux: web shell detection, file protection, HIPS detection, login security check, malicious file detection, abnormal process behaviors, root privilege escalation, real-time process, and rootkit detection – Windows: AV detection, web shell detection, HIPS detection, login security check, and real-time process ● Premium/WTP edition – Linux: cluster intrusion detection, web shell detection, file protection, HIPS detection, login security check, malicious file detection, port scan detection, abnormal process behaviors, root privilege escalation,

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
					real-time process, and rootkit detection – Windows: AV detection, web shell detection, HIPS detection, login security check, and real-time process ● Container edition Cluster intrusion detection, container escape detection, web shell detection, container file monitoring, container process whitelist, and suspicious image behaviors
	Login security policy not enabled	All	10	×	In HSS professional, enterprise, premium, WTP, and container editions, you need to enable the **Login Security Check** policy for servers. For details, see **Overview**.
	Ransomware prevention policy not enabled	Premium edition	15	×	The HSS premium, WTP, and container editions support ransomware prevention. In these editions, you need to enable the ransomware prevention policy and the backup policy. (10 points will be deducted if backup is not enabled.) For details, see **Enabling Ransomware Prevention**.
	WTP policy is not enabled	WTP edition	20	×	In the HSS WTP edition, you need to enable WTP policy for servers. For details, see **Enabling Web Tamper Protection**.

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
	Container runtime detection policy not enabled	Container edition	20	×	In the HSS container edition, you need to enable container escape, container process whitelist, container file monitoring, and container information collection policies and apply them to servers. For details, see **Overview**.

Table 2-5 Asset risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Open ports	Open TCP/UDP high-risk ports	All	1	√	You are advised to disable unnecessary ports. To enable a port, choose **Asset Management** > **Server Fingerprints**, click **Open Ports**, and ignore the port.
Asset discovery not enabled	Asset discovery policy not enabled	All	5	×	● The HSS basic, professional, and enterprise editions do not provide asset discovery. To use this feature, upgrade HSS to the premium edition. For details, see **Upgrading Protection Quotas**. ● In the HSS premium and WTP editions, you are advised to enable the **Asset Discovery** policy. For details, see **Overview**.

Table 2-6 Image risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unsafe images	High-risk images	Container edition	3	√	Re-create an image, scan the image, and update the score.
	Medium-risk images	Container edition	1	√	
	Medium-risk images	Container edition	0.1	√	
Image security scan not performed	No image security scans were performed in the past month.	Container edition	5	×	In the HSS container edition, you are advised to perform image security scans. For details, see **Container Images**.

Table 2-7 Unprotected assets risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Server protection not enabled	Unprotected servers	All	0.1–1	√	The points deducted for an unprotected server vary depending on its asset importance: ● Important asset: 1 ● General asset: 0.5 ● Test asset: 0.1 You are advised to enable protection for your server as soon as possible. For details, see **Enabling Protection**.

3 Asset Management

3.1 Asset Management

You can count all your assets and check their statistics, including the agent status, protection status, quota, account, port, process, software, and auto-started items.

Constraints

Servers that are not protected by HSS do not support the asset overview function.

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** > **HSS**.

Step 3 Choose **Asset Management** > **Assets**. Check your assets and their statistics.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

- **Asset Types**: Displays the number of server and container nodes. You can click an asset type in the ring chart to go to the corresponding asset list page.
- **Agent Status**: displays the number of servers in the **Online**, **Offline**, and **Not installed** states. You can click an agent status in the ring chart to go to the corresponding server list page.
- **Servers**: Displays the number of unprotected and protected servers. You can click a server type in the ring chart to go to the corresponding server list page.
- **Containers**: Displays the number of unprotected and protected container nodes. You can click a container type in the ring chart to go to the corresponding container node list page.
- **Quotas**: Displays the protected quota types and their usage status. You can click **Protected Servers** or **Protected Containers** to go to the corresponding protected quota list page.

- **OS Types**: Displays the number and proportion of OS types. You can click an OS type in the ring chart to go to the corresponding server list page.
- Assets: Displays asset information, including account information, open ports, processes, installed software, auto-startup items, web applications, web services, web frameworks, websites, middleware, databases, and kernel modules. You can click the value of each asset item to go to the corresponding asset list page.

----End

3.2 Server Fingerprints

3.2.1 Collecting Server Asset Fingerprints

HSS can collect server asset fingerprints, including information about ports, processes, web applications, web services, web frameworks, and auto-started items. You can centrally check server asset information and detect risky assets in a timely manner based on the server fingerprints. This section describes server asset fingerprints and their collection method.

Prerequisite

HSS enterprise edition, premium edition, WTP edition, or container edition has been enabled for the server.

Server Asset Fingerprint Collection Items

Table 3-1 lists the collection items of server asset fingerprints. Each asset fingerprint is automatically collected periodically. If you are using HSS premium edition or later, you can customize the asset fingerprint collection period. For details, see **Asset Discovery**.

Table 3-1 Asset fingerprints

Item	Description	Supported OS	Automatic Detection Period
Account Information	Check and manage all accounts on your servers to keep them secure. You can check real-time and historical account information to find suspicious accounts. ● Real-time account information includes the account name, number of servers, server name/IP address, login permission, root permission, user group, user directory, shell started by the user, and the last scan time. ● Historical account change records include the server name/IP address, change status, login permission, root permission, user group, user directory, shell started by the user, and the last scan time.	Linux and Windows	Automatic check every hour
Open Ports	Check open ports on your servers, including risky and unknown ports. You can easily identify high-risk ports by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files. ● 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 at the **Dangerous** risk level promptly and handle the ports at 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.	Linux and Windows	Automated check every 30 seconds

Item	Description	Supported OS	Automatic Detection Period
Processes	Check processes on your servers and find abnormal processes. You can easily identify abnormal processes based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes. If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.	Linux and Windows	Automatic check every hour
Installed Software	Check and manage all software installed on your containers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. ● Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, and the last scan time. ● Historical software change records include the server names, IP addresses, change statuses, software versions, software update time, and the last scan time.	Linux and Windows	Automatic check every day
Auto-startup	Check for auto-startup items and quickly locate Trojans. ● Real-time information about auto-started items includes their names, types (auto-started service, startup folder, pre-loaded dynamic library, Run registry key, or scheduled task), number of servers, server names, IP addresses, paths, file hashes, users, and the last scan time. ● The historical change records of auto-started items include server names, IP addresses, change statuses, paths, file hashes, users, and the last scan time.	Linux and Windows	Automatic check every hour

Item	Description	Supported OS	Automatic Detection Period
Websites	You can check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, certificate information (to be provided later), and key processes of websites.	Linux	Once a week (04:10 a.m. every Monday)
Web Frameworks	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	Linux	Once a week (04:10 a.m. every Monday)
Middleware	You can check information about servers, versions, paths, and processes associated with middleware.	Linux and Windows	Once a week (04:10 a.m. every Monday)
Kernel Module	You can check information about all the program module files running in kernels, including associated servers, version numbers, module descriptions, driver file paths, file permissions, and file hashes.	Linux	Once a week (04:10 a.m. every Monday)
Web Services	You can check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software.	Linux	Once a week (04:10 a.m. every Monday)
Web Applications	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software.	Linux and Windows (only Tomcat is supported)	Once a week (04:10 a.m. every Monday)

Item	Description	Supported OS	Automatic Detection Period
Databases	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software.	Linux and Windows (only MySQL is supported)	Once a week (04:10 a.m. every Monday)

Collecting the Latest Asset Fingerprints of a Single Server

If you want to obtain the latest data of assets such as web applications, web services, web frameworks, websites, middleware, kernel modules, and databases, in real time, you can manually collect fingerprint 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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Servers**.

Step 5 Click a fingerprint in the fingerprint list, and click **Discover Assets** on the upper area of the list on the right.

NOTE

Currently, only the information about web applications, web services, web frameworks, websites, middleware, kernel modules, and databases can be manually collected and updated in real time. Information about other types is automatically collected and updated every day.

Step 6 After the automatic execution is complete, the last scan time is updated and the latest server asset information is displayed.

----End

3.2.2 Viewing Server Asset Fingerprints

HSS can collect server asset fingerprints, including information about ports, processes, web applications, web services, web frameworks, and auto-started items. You can centrally check server asset information and detect risky assets in a timely manner based on the server fingerprints. This section describes how to view collected server asset fingerprints on the console.

Prerequisite

HSS enterprise edition, premium edition, WTP edition, or container edition has been enabled for the server.

Viewing Asset Information of All 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** > **HSS**.

Step 3 Choose **Asset Management** > **Server Fingerprints** to view all server assets.

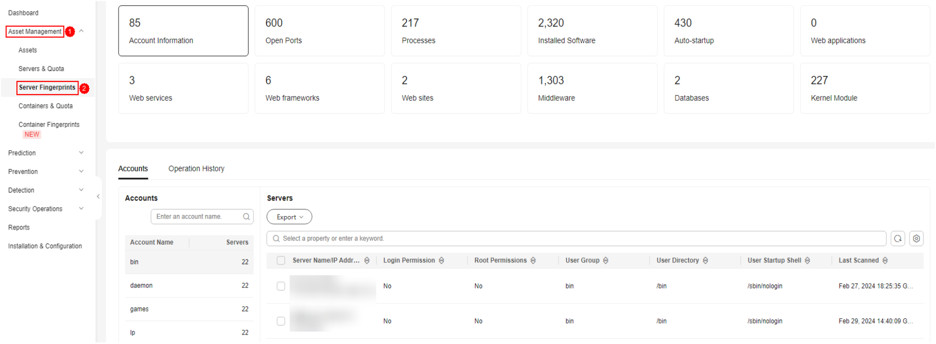
Delete risky assets in a timely manner. Common high-risk ports are listed in the **High-risk port list**. You are advised to handle the ports as follows:

- If HSS detects open high-risk ports or unused ports, check whether they are really used by your services.
- 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.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 3-1 Viewing server asset information



85 Account Information	600 Open Ports	217 Processes	2,320 Installed Software	430 Auto-startup	0 Web applications
3 Web services	6 Web frameworks	2 Web sites	1,303 Middleware	2 Databases	227 Kernel Module

Accounts

Account Name	Servers
bin	22
daemon	22
games	22
lp	22

Servers

Server Name/IP Addr...	Login Permission	Root Permissions	User Group	User Directory	User Startup Shell	Last Scanned
[redacted]	No	No	bin	/bin	/sbin/nologin	Feb 27, 2024 18:25:35 G...
[redacted]	No	No	bin	/bin	/sbin/nologin	Feb 29, 2024 14:40:09 G...

Table 3-2 Asset fingerprints

Item	Description	Supported OS	Automatic Detection Period
Account Information	Check and manage all accounts on your servers to keep them secure. You can check real-time and historical account information to find suspicious accounts. ● Real-time account information includes the account name, number of servers, server name/IP address, login permission, root permission, user group, user directory, shell started by the user, and the last scan time. ● Historical account change records include the server name/IP address, change status, login permission, root permission, user group, user directory, shell started by the user, and the last scan time.	Linux and Windows	Automatic check every hour
Open Ports	Check open ports on your servers, including risky and unknown ports. You can easily identify high-risk ports by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files. ● 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 at the **Dangerous** risk level promptly and handle the ports at 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.	Linux and Windows	Automated check every 30 seconds

Item	Description	Supported OS	Automatic Detection Period
Processes	Check processes on your servers and find abnormal processes. You can easily identify abnormal processes based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes. If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.	Linux and Windows	Automatic check every hour
Installed Software	Check and manage all software installed on your containers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. ● Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, and the last scan time. ● Historical software change records include the server names, IP addresses, change statuses, software versions, software update time, and the last scan time.	Linux and Windows	Automatic check every day
Auto-startup	Check for auto-startup items and quickly locate Trojans. ● Real-time information about auto-started items includes their names, types (auto-started service, startup folder, pre-loaded dynamic library, Run registry key, or scheduled task), number of servers, server names, IP addresses, paths, file hashes, users, and the last scan time. ● The historical change records of auto-started items include server names, IP addresses, change statuses, paths, file hashes, users, and the last scan time.	Linux and Windows	Automatic check every hour

Item	Description	Supported OS	Automatic Detection Period
Websites	You can check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, certificate information (to be provided later), and key processes of websites.	Linux	Once a week (04:10 a.m. every Monday)
Web Frameworks	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	Linux	Once a week (04:10 a.m. every Monday)
Middleware	You can check information about servers, versions, paths, and processes associated with middleware.	Linux and Windows	Once a week (04:10 a.m. every Monday)
Kernel Module	You can check information about all the program module files running in kernels, including associated servers, version numbers, module descriptions, driver file paths, file permissions, and file hashes.	Linux	Once a week (04:10 a.m. every Monday)
Web Services	You can check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software.	Linux	Once a week (04:10 a.m. every Monday)
Web Applications	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software.	Linux and Windows (only Tomcat is supported)	Once a week (04:10 a.m. every Monday)

Item	Description	Supported OS	Automatic Detection Period
Databases	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software.	Linux and Windows (only MySQL is supported)	Once a week (04:10 a.m. every Monday)

----End

Viewing Asset Information of a Single 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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

> NOTE
>
> If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Servers**.

Step 5 Click a fingerprint in the fingerprint list to view its asset information. For more information, see **Table 3-2**.

----End

High-risk port list

Table 3-3 lists the high-risk ports are identified by the asset fingerprint function of HSS. If a high-risk port is enabled in your asset, check whether they are really used by your services.

Table 3-3 High-risk port list

Port	Description	Protocol
31	Trojan horses Master Paradise and Hackers Paradise	TCP and UDP
456	Trojan horses HACKERSPARADISE	TCP and UDP

Port	Description	Protocol
555	Trojan horses PhAse1.0 Stealth Spy and IniKiller	TCP and UDP
666	Trojan horses Attack FTP and Satanz Backdoor	TCP and UDP
1001	Trojan horses Silencer and WebEx	TCP and UDP
1011	Trojan horse Doly Trojan	TCP and UDP
1025	Trojan horse netspy	TCP and UDP
1033	Trojan horse netspy	TCP and UDP
1070	Trojan horses Streaming Audio Trojan Psyber Stream Server and Voice	TCP and UDP
1234	Trojan horses SubSeven2.0 and Ultors Trojan	TCP and UDP
1243	Trojan horse SubSeven 1.0/1.9	TCP and UDP
1245	Trojan horse Vodoo	TCP and UDP
1270	MOM-Encrypted Microsoft Operations Manager (MOM) 2000	TCP
1492	Trojan horse FTP99CMP	TCP and UDP
1600	Trojan horse Shivka-Burka	TCP and UDP
1807	Trojan horse SpySender	TCP and UDP
1981	Trojan horse ShockRave	TCP and UDP
1999	Trojan horse BackDoor	TCP and UDP
2000	Trojan horses GirlFriend 1.3 and Millenium 1.0	TCP and UDP
2001	Trojan horses Millenium 1.0 and Trojan Cow	TCP and UDP
2023	Trojan horse Pass Ripper	TCP and UDP
2115	Trojan horse Bugs	TCP and UDP
2140	Trojan horse Deep Throat 1.0/3.0	TCP and UDP
3150	Trojan horse Deep Throat 1.0/3.0	TCP and UDP
6711	Trojan horse SubSeven1.0/1.9	TCP and UDP
6776	Trojan horses SubSeven2.0 and Ultors Trojan and SubSeven1.0/1.9	TCP and UDP

3.2.3 Viewing the Operation History of Server Assets

HSS proactively records the changes on account information, software information, and auto-started items. You can check the change details according to different dimensions and time ranges.

Prerequisite

HSS enterprise edition, premium edition, WTP edition, or container edition has been enabled for the server.

Checking Change Records

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** > **HSS**.

Step 3 Choose **Asset Management** > **Server Fingerprints** and click **Operation History**. On the displayed **Operation History** page, select a dimension and time period to view the change history of accounts, software, and auto-started items.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

----End

Managing Account Information

Account changes are recorded.

- **Action**: 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).
- **Last Scan Time**: The last scan time indicates the time of the latest scan performed for servers in a period.

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.

Managing Software

Operations made to accounts are recorded.

- **Action**: **Create** and **Delete**.
- **Last Scan Time**: The last scan time records the time when the changes were detected, not the time 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.

Auto-started Items

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, IP addresses, changes, paths, file hashes, users, and last scan time of auto-startup items.

3.3 Container Fingerprints

3.3.1 Collecting Container Asset Fingerprints

HSS can collect container asset fingerprints, including container clusters, services, workloads, accounts, ports, and processes. You can centrally check container asset information and detect risky assets in a timely manner based on the container fingerprints. This section describes how to collect container asset fingerprints.

Prerequisite

HSS container edition has been enabled for the server.

Container Asset Fingerprint Collection Items

Table 3-4 lists the collection items of container asset fingerprints. The fingerprint items except clusters, services, workloads, and container instances are automatically collected periodically. You can customize the asset fingerprint collection period. For details, see **Asset Discovery**.

Table 3-4 Container asset fingerprints

Item	Description	Automatic Detection Period
Account Information	Check and manage all accounts on your containers to keep them secure. Real-time account information includes the account name, number of servers, server name, IP address, login permission, root permission, user group, user directory, shell started by the user, container name, container ID, and the last scan time.	Automatic check every hour

Item	Description	Automatic Detection Period
Open Ports	Check open ports on your containers, including risky and unknown ports. You can easily find high-risk ports on containers by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files. ● 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.	Automated check every 30 seconds
Processes	Check processes on your containers and find abnormal processes. You can easily identify abnormal processes on your containers based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes. If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.	Automatic check every hour
Installed Software	Check and manage all software installed on your containers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. ● Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, and the last scan time. ● Historical software change records include the server names, IP addresses, change statuses, software versions, software update time, and the last scan time.	Automatic check every day

Item	Description	Automatic Detection Period
Auto-startup	Check for auto-started items and quickly locate Trojans. Real-time information about auto-started items includes their names, types (auto-started service, startup folder, pre-loaded dynamic library, Run registry key, or scheduled task), number of servers, server names, IP addresses, paths, file hashes, users, container name, container ID, and the last scan time.	Automatic check every hour
Websites	You can check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, certificate information (to be provided later), and key processes of websites.	Once a week (04:10 a.m. every Monday)
Web Framework	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	Once a week (04:10 a.m. every Monday)
Middleware	You can also check information about servers, versions, paths, and processes associated with middleware.	Once a week (04:10 a.m. every Monday)
Web Services	You can check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software.	Once a week (04:10 a.m. every Monday)
Web Applications	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software.	Once a week (04:10 a.m. every Monday)
Databases	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software.	Once a week (04:10 a.m. every Monday)
Clusters	Collect statistics on and display cluster details. You can view the type, node, version, and status of all clusters.	-
Services	Collect statistics on and display details about services and breakpoints. You can view information about all services, such as namespaces and clusters to which the services belong.	-

Item	Description	Automatic Detection Period
Workloads	Collect statistics on and display details about workloads (StatefulSets, deployments, DaemonSets, normal jobs, cron jobs, and container groups). You can view the status, number of instances, and namespace of all workloads.	-
Pods	Collect statistics on and display container instance details. You can view the status, POD, and cluster of all container instances.	-

Collecting the Latest Asset Fingerprints of a Single Container

If you want to view the latest data of assets such as web applications, web services, web frameworks, websites, middleware, and databases in real time, you can manually collect the fingerprint 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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Containers**.

Step 5 Click a fingerprint in the fingerprint list, and click **Discover Assets** on the upper area of the list on the right.

NOTE

Currently, only **Web Applications**, **Web Services**, **Web Frameworks**, **Websites**, **Middleware**, and **Databases** support real-time manual collection and update. Information about other types is automatically collected and updated every day.

Step 6 After the automatic execution is complete, the last scan time is updated and the latest container asset information is displayed.

----End

Collecting Clusters, Services, Workloads, and Containers Information

The information about clusters, services, workloads, and containers is not collected automatically. If your assets change, manually collect the latest data referring to this section.

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

----End

3.3.2 Viewing Container Asset Fingerprints

HSS can collect container asset fingerprints, including container clusters, services, workloads, accounts, ports, and processes. You can centrally check container asset information and detect risky assets in a timely manner based on the container fingerprints. This section describes how to view collected container asset information.

Constraints

- Only the HSS container edition supports the container fingerprint function.
- Only Linux is supported.

Viewing Asset Fingerprints Data of All Containers

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** > **HSS**.

Step 3 Choose **Asset Management** > **Container Fingerprints** > **Asset Fingerprints**. On the **Asset Fingerprints** page that is displayed, view the fingerprint data of all containers.

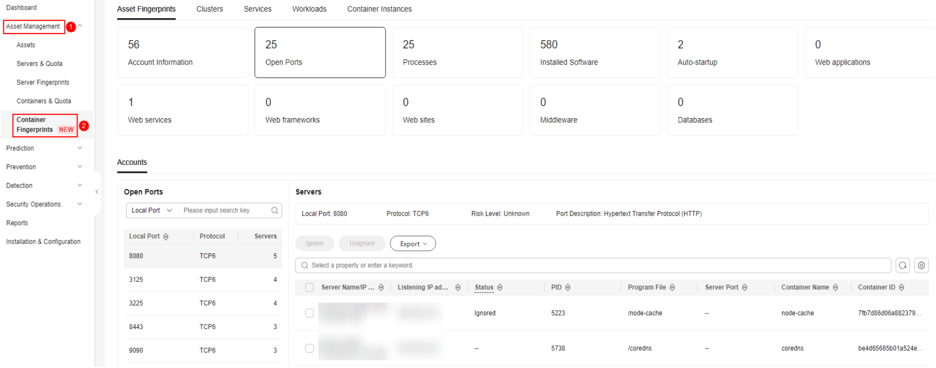
If you find risky assets after counting, remove them in a timely manner. Common high-risk ports are listed in the **High-risk port list**. You are advised to handle the ports as follows:

- If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. If they are not, disable them. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.
- If a detected high-risk port is actually a normal port used for services, you can ignore it. Ignored alarms will neither be recorded as unsafe items and nor trigger alarms.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 3-2 Viewing container assets



Local Port: 8080 Protocol: TCP6 Risk Level: Unknown Port Description: Hypertext Transfer Protocol (HTTP)

Local Port	Protocol	Servers
8080	TCP6	5
3125	TCP6	4
3225	TCP6	4
8443	TCP6	3
9090	TCP6	3

Server Name/IP ...	Listening IP ad...	Status	PID	Program File	Server Port	Container Name	Container ID
[redacted]	[redacted]	Ignored	5223	/node-cache	--	node-cache	7fb7d86d06a882379...
[redacted]	[redacted]	--	5738	/coredns	--	coredns	be4d65665b01a524e...

Table 3-5 Container asset fingerprints

Item	Description	Automatic Detection Period
Account Information	Check and manage all accounts on your containers to keep them secure. Real-time account information includes the account name, number of servers, server name, IP address, login permission, root permission, user group, user directory, shell started by the user, container name, container ID, and the last scan time.	Automatic check every hour
Open Ports	Check open ports on your containers, including risky and unknown ports. You can easily find high-risk ports on containers by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files. ● 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.	Automated check every 30 seconds

Item	Description	Automatic Detection Period
Processes	Check processes on your containers and find abnormal processes. You can easily identify abnormal processes on your containers based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes. If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.	Automatic check every hour
Installed Software	Check and manage all software installed on your containers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. ● Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, and the last scan time. ● Historical software change records include the server names, IP addresses, change statuses, software versions, software update time, and the last scan time.	Automatic check every day
Auto-startup	Check for auto-started items and quickly locate Trojans. Real-time information about auto-started items includes their names, types (auto-started service, startup folder, pre-loaded dynamic library, Run registry key, or scheduled task), number of servers, server names, IP addresses, paths, file hashes, users, container name, container ID, and the last scan time.	Automatic check every hour
Websites	You can check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, certificate information (to be provided later), and key processes of websites.	Once a week (04:10 a.m. every Monday)
Web Framework	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	Once a week (04:10 a.m. every Monday)

Item	Description	Automatic Detection Period
Middleware	You can also check information about servers, versions, paths, and processes associated with middleware.	Once a week (04:10 a.m. every Monday)
Web Services	You can check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software.	Once a week (04:10 a.m. every Monday)
Web Applications	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software.	Once a week (04:10 a.m. every Monday)
Databases	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software.	Once a week (04:10 a.m. every Monday)
Clusters	Collect statistics on and display cluster details. You can view the type, node, version, and status of all clusters.	-
Services	Collect statistics on and display details about services and breakpoints. You can view information about all services, such as namespaces and clusters to which the services belong.	-
Workloads	Collect statistics on and display details about workloads (StatefulSets, deployments, DaemonSets, normal jobs, cron jobs, and container groups). You can view the status, number of instances, and namespace of all workloads.	-
Pods	Collect statistics on and display container instance details. You can view the status, POD, and cluster of all container instances.	-

----End

Viewing Asset Fingerprint Data of a Single Container

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the name of the target server. On the server details page that is displayed, click the **Asset Fingerprints** > **Containers** tab.

Step 5 Click a fingerprint in the fingerprint list to view its asset information.

----End

Viewing Cluster 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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 6 On the **Clusters** page, view cluster information.

The **Clusters** page displays the cluster name, type, node, version, creation time, and status.

- Searching for the target cluster

  You can enter information such as the cluster name and status in the search box and click 🔍 to search for the target cluster.

- Viewing details about the target cluster

  a. Click the name of the target cluster to go to the CCE console.

  b. On the CCE console, view basic cluster information and network information.

----End

Viewing Services

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 6 On the **Services** tab page, view the information.

The page displays the service name, endpoint name, access mode, service IP address, namespace, cluster, and creation time.

- Searching for a service

  You can enter information such as the service name and access mode in the search box and click 🔍 to search for the service.
- Viewing details about a service

  Click the name of a service. On the service details page that is displayed, you can view the selector, tag, and port of the service.

----End

Viewing Endpoints

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 6 Choose **Services** > **Endpoints**. View endpoints information.

The page displays the endpoint name, namespace, cluster, associated with service, service name, and creation time.

- Searching for an endpoint

  You can enter information such as the endpoint name and namespace in the search box and click 🔍 to search for the endpoint.
- Viewing details about an endpoint

  Click the name of an endpoint. On the endpoint details page that is displayed, you can view the pod mapping and port information.

----End

Viewing a Workload

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 6 Click the **Workloads** tab.

Step 7 Select different workloads and view information.

You can view information about **Deployment**, **StatefulSets**, **DaemonSets**, **Jobs**, **Cron Jobs**, and **Pods**. For details about the information items, see **Workload information Items**.

You can enter information such as the workload name and cluster in the search box and click 🔍 to search for the target workload.

Table 3-6 Workload information

Workload Type	Item
Deployment	• Workload name • Status • Instances • Namespaces • Created • Image name • Cluster
StatefulSets	• Workload name • Status • Instances • Namespace • Created • Image name • Cluster
DaemonSets	• Workload name • Status • Instances • Namespace • Created • Image name • Cluster
Jobs	• Workload name • Status • Instances • Namespace • Created • Image name • Cluster

Workload Type	Item
Cron Jobs	• Workload name • Status • Trigger • Running jobs • Namespace • Latest scheduled • Created • Image name • Cluster
Pods	• Name • Namespace • Cluster • Node • Pod IP address • POD IP • Status • Created

----End

Viewing Container Instances

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 6 Click the **Container Instances** tab.

The container name, status, pod, cluster, creation time, and image name are displayed.

- Searching for a container

  You can enter information such as the container name and status in the search box and click 🔍 to search for the container.

- Viewing details about a container

Click the name of a container. On the container details page that is displayed, you can view the process, port, and mount path.

----End

3.4 Server Management

3.4.1 Viewing Server Protection Status

You are advised to periodically check the server protection status and handle security risks in a timely manner to prevent asset loss.

The server list on the **Servers & Quota** 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 Server Protection Status

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. The HSS console is displayed.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. On the **Servers** tab, view the protection status of the server. For more information, see **Table 3-7**.

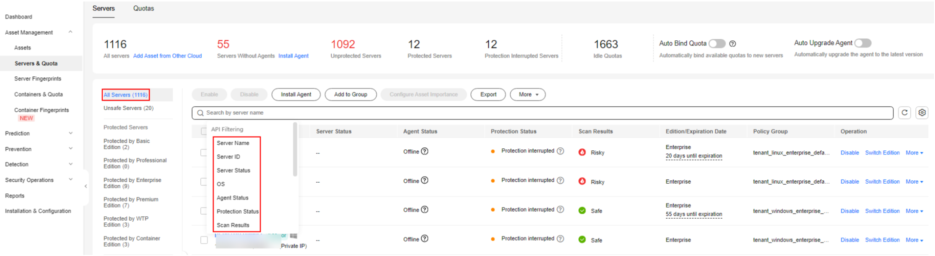
NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

You can check the server name, ID, IP address, OS, running status, and enterprise project. To set the items to be displayed in the server protection list, click ⚙ in the upper right corner.

- To check the protection status of a server, enter a server name, server ID, or IP address in the search box above the server protection list, and click 🔍.

Figure 3-3 Searching for a protected server



1116 All servers Add Asset from Other Cloud

55 Servers Without Agents Install Agent

1092 Unprotected Servers

12 Protected Servers

12 Protection Interrupted Servers

1663 Idle Quotas

Auto Bind Quota: Automatically bind available quotas to new servers

Auto Upgrade Agent: Automatically upgrade the agent to the latest version

Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Policy Group	Operation
--	Offline	Protection interrupted	Risky	Enterprise 20 days until expiration	tenant_linux_enterprise_defa...	Disable Switch Edition More
--	Offline	Protection interrupted	Risky	Enterprise	tenant_linux_enterprise_defa...	Disable Switch Edition More
--	Offline	Protection interrupted	Safe	Enterprise 55 days until expiration	tenant_windows_enterprise_...	Disable Switch Edition More
--	Offline	Protection interrupted	Safe	Enterprise	tenant_windows_enterprise_...	Disable Switch Edition More

- On the left of the server protection list, select a server protection edition or an asset importance category to view the protection status of each type of servers.

Table 3-7 Protection status description

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. **NOTE** The server information will be automatically deleted from the server management page after the agent goes offline for 30 days.
Protection Status	● **Enabled**: The server is fully protected by HSS. ● **Unprotected**: HSS is disabled for the server. After the agent is installed, click **Enable** in the **Operation** column to enable protection. ● **Protection interrupted**: The server is shut down, the agent is offline, or the agent is uninstalled.
Scan Results	● **Risky**: The host has risks. ● **Safe**: No risks are found. ● **Pending risk detection**: HSS is not enabled for the server.

----End

Viewing the WTP Status

Step 1 Log in to the management console and go to the HSS page.

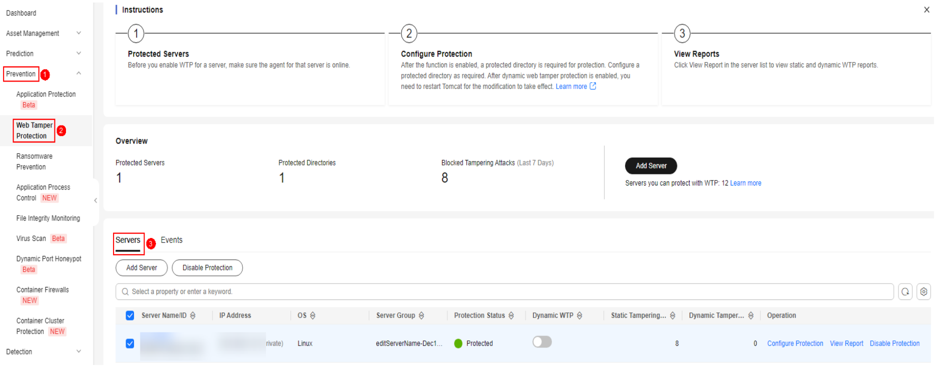
Step 2 Choose **Prevention** > **Web Tamper Protection** and click **Servers** to view the protection status of the servers.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

To check the protection status of a target server, enter a server name, server ID, or IP address in the search box above the protection list, and click 🔍.

Figure 3-4 Servers protected by WTP



Protected Servers
Before you enable WTP for a server, make sure the agent for that server is online.

Configure Protection
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

View Reports
Click View Report in the server list to view static and dynamic WTP reports.

Protected Servers: 1
Protected Directories: 1
Blocked Tampering Attacks (Last 7 Days): 8

Servers you can protect with WTP: 12 Learn more

☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑	[redacted]	[redacted]rivate)	Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Table 3-8 Statuses

Parameter	Description
Protection Status	**Protected**: HSS provides static web tamper protection (WTP) for the server.
Dynamic WTP	Status of dynamic WTP, which can be: ● (on): Dynamic WTP is enabled. ● (off): Dynamic WTP is disabled. (After enabling dynamic WTP, restart Tomcat to make this setting take effect.)
Static Tampering Attacks	Number of times that static web page files are attacked and tampered with.
Dynamic Tampering Attacks	Number of web application vulnerability exploits and injection attacks.

----End

3.4.2 Disabling Protection

3.4.2.1 Disabling the Basic/Professional/Enterprise/Premium Edition

You can disable protection for a server. A quota that has been unbound from a server can be bound to another one.

Precautions

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

To unsubscribe from the pay-per-use quota of the enterprise edition, you just need to disable the protection.

Disabling 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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

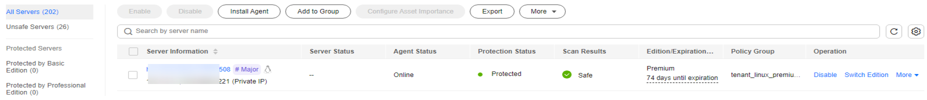
NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Disable protection for one or multiple servers.

- **Disabling protection for a server**
  a. Click **Disable** in the **Operation** column of a server.

Figure 3-5 Disabling protection for a server



☐	Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration...	Policy Group	Operation
☐	[redacted] 508 # Major [redacted] 221 (Private IP)	--	Online	● Protected	✓ Safe	Premium 74 days until expiration	tenant_linux_premiu...	Disable Switch Edition More ▾

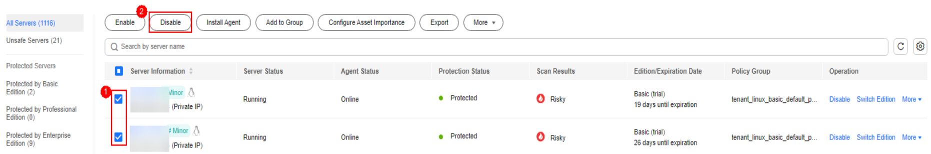
  b. In the dialog box that is displayed, confirm the information and click **OK**.
  c. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

CAUTION

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

- **Disabling protection in batches**
  a. Select multiple servers and click **Disable** above the server list.

Figure 3-6 Disabling protection in batches


All Servers (1116)
Unsafe Servers (21)
Protected Servers
Protected by Basic Edition (2)
Protected by Professional Edition (0)
Protected by Enterprise Edition (9)
2
Enable
Disable
Install Agent
Add to Group
Configure Asset Importance
Export
More ▾
Search by server name
1

☑	Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Policy Group	Operation
☑	[redacted] Minor (Private IP)	Running	Online	● Protected	Risky	Basic (trial) 19 days until expiration	tenant_linux_basic_default_p...	Disable Switch Edition More ▾
☑	[redacted] Minor (Private IP)	Running	Online	● Protected	Risky	Basic (trial) 26 days until expiration	tenant_linux_basic_default_p...	Disable Switch Edition More ▾

  b. In the dialog box that is displayed, confirm the information and click **OK**.

c. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

> ⚠ CAUTION
>
> Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

----End

3.4.2.2 Disabling WTP

You can disable the WTP edition for a server. A quota that has been unbound from a server can be bound to another one.

Precautions

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

Procedure

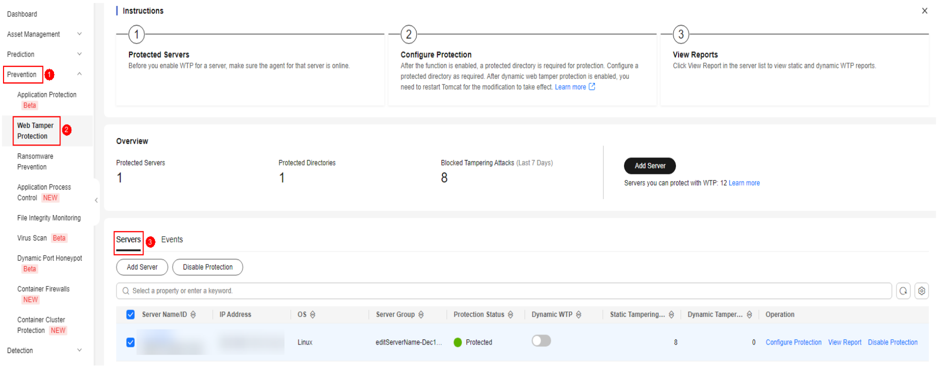
Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Protection** > **Web Tamper Protection**. On the **Web Tamper Protection** page, click the **Servers** tab.

> 🕮 NOTE
>
> If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 3-7 Entering the page for protected directory settings



Protected Servers
Before you enable WTP for a server, make sure the agent for that server is online.

Configure Protection
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

View Reports
Click View Report in the server list to view static and dynamic WTP reports.

Protected Servers 1
Protected Directories 1
Blocked Tampering Attacks (Last 7 Days) 8

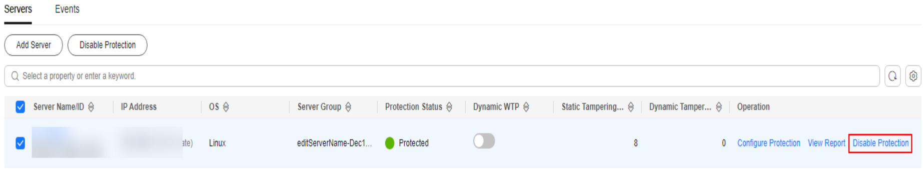
Servers you can protect with WTP: 12 Learn more

☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑	[redacted]	[redacted]	Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 4 Click **Disable** in the **Operation** column of a server.

You can also select multiple servers, and click **Disable** above the server list to disable protection in batches.

Figure 3-8 Disabling WTP



☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑	[redacted]	[redacted]ate)	Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 5 In the dialog box that is displayed, confirm the information and click **OK**.

Step 6 Choose **Asset Management** > **Servers & Quota** and click the **Servers** tab. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

CAUTION

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

----End

3.4.3 Exporting the Server List

This section describes how to export the server protection list to your local PC.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 In the upper right corner of the server list, click **Export** to export the server list details.

You can also select specified servers in the server list and click **Export**.

NOTE

The details of up to 1,000 servers can be exported at a time.

----End

3.4.4 Switching the HSS Quota Edition

You can switch the quota edition of a server to the basic, professional, enterprise, or premium edition as needed.

Precautions

You can switch to the basic, professional, enterprise or premium edition.

To use the WTP or container edition, purchase a quota of that edition and then enable it. For details, see **Purchasing an HSS Quota**.

Prerequisites

- The server whose protection quota is to be changed is in the **Protected** state.
- Before switching to a quota in yearly/monthly billing mode, ensure the quota has been purchased and is available. For details, see **Purchasing an HSS Quota**.
- Before switching to a lower edition, check the server, handle known risks, and record operation information to prevent O&M errors and attacks.

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

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 You can switch the quota editions for one or multiple servers.

- Switching the quota edition for a single server
  a. In the **Operation** column of a server, click **Switch Edition**.
  b. In the **Configure Protection** area, select a billing mode, an edition, and a quota. For more information, see **Table 3-9**. For details about the editions that can be switched, see **Table 3-10**.

Table 3-9 Parameters for switching editions

Parameter	Description
Billing Mode	Billing mode of a quota. ▪ Yearly/Monthly ▪ Pay-per-use

Parameter	Description
Edition	Select a quota edition. ▪ Basic edition: It protects test servers or individual users' servers. **It 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 the DJCP Multi-level Protection Scheme (MLPS) certification**. The basic edition is free of charge for 30 days if it was enabled for the first time. ▪ Professional edition: This edition is higher than the basic edition but lower than the enterprise edition. Its features include file directory change detection, abnormal shell detection, and policy management. ▪ Enterprise edition: It provides assistance for the DJCP MLPS certification. Main features include asset fingerprint management, vulnerability management, malicious program detection, web shell detection, and abnormal process behavior detection. ▪ Premium edition: It helps you with the DJCP MLPS certification and provides advanced features, including application protection, ransomware prevention, high-risk command detection, privilege escalation detection, and abnormal shell detection. For more information, see **Editions and Features**.
Select Quota	If you select **Yearly/Monthly**, you need to select a protection quota for the server. ▪ **Select a quota randomly**: A random quota is allocated to the server. ▪ Quota ID: The specified quota is bound to the server. When you switch the edition for multiple servers at a time, the quota you select can only be bound to one of them. The rest of the servers will be randomly bound to the quotas of the target edition. **NOTE** If the system displays a message indicating that there are no available quotas, you need to purchase quotas first.
Tags (optional)	If you select the pay-per-use billing mode, you can add tags to pay-per-use quotas. Tags are used to identify cloud resources. When you have many cloud resources of the same type, you can use tags to classify cloud resources by dimension (for example, by usage, owner, or environment).

Table 3-10 Allowed edition switching

Billing Mode	Current Edition	Allowed Target Edition
Yearly/ Monthly	Basic	■ Yearly/Monthly: professional, enterprise, and premium editions ■ Pay-per-use: enterprise edition
	Professional edition	■ Yearly/Monthly: basic, enterprise, and premium editions ■ Pay-per-use: enterprise edition
	Enterprise	Yearly/Monthly: basic, professional, and premium editions
	Premium	■ Yearly/Monthly: basic, professional, and enterprise editions ■ Pay-per-use: enterprise edition
Pay-per-use	Enterprise	Yearly/Monthly: basic, professional, and premium editions

c. Read the *Host Security Service Disclaimer* and select **I have read and agree to the Host Security Service Disclaimer**.

- Switching the quota editions for multiple servers
  a. Select multiple servers and click **Enable** above the server list.
  b. In the dialog box that is displayed, confirm the server information and select a billing mode, an edition, and a quota. For more information, see **Table 3-9**.
  c. Read the *Host Security Service Disclaimer* and select **I have read and agree to the Host Security Service Disclaimer**.

Step 5 Click **OK**.

The edition information in the **Edition** column will be updated. If the edition information in the **Edition** column is updated, the HSS edition switch succeeded.

----End

Follow-up Procedure

- After the edition is switched, you can allocate the idle edition quota to other servers.
- 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, perform a security detection on the server, handle security risks on the server, and configure necessary functions in a timely manner.

3.4.5 Deploying a Protection 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 the professional, enterprise, premium, WTP, or container edition is enabled, the protection policy group of the corresponding edition is deployed by default and applies to servers. You do not need to manually deploy policies. For premium and container editions, you can copy a policy group and customize it as required. To flexibly manage server protection policies, you can replace the default policy group with a custom policy group.

Creating a Policy 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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Security Operations** > **Policies**

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

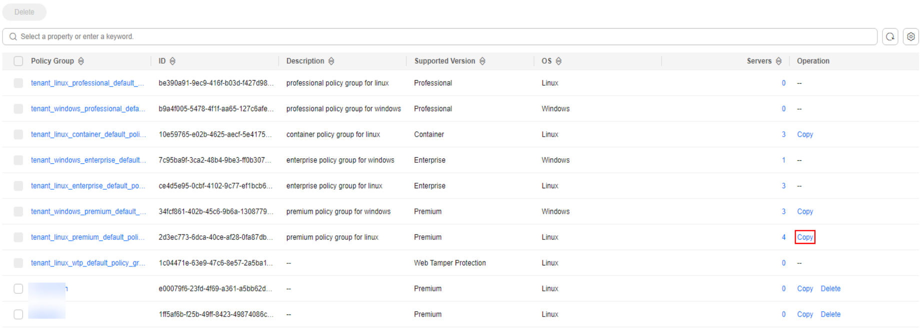
Step 4 Copy a policy group.

NOTE

Currently, only policies of premium and container editions can be copied.

- Select the **tenant_linux_premium_default_policy_group** policy group. Locate the row that this policy group resides, click **Copy** in the **Operation** column.

Figure 3-9 Copying a Linux policy group



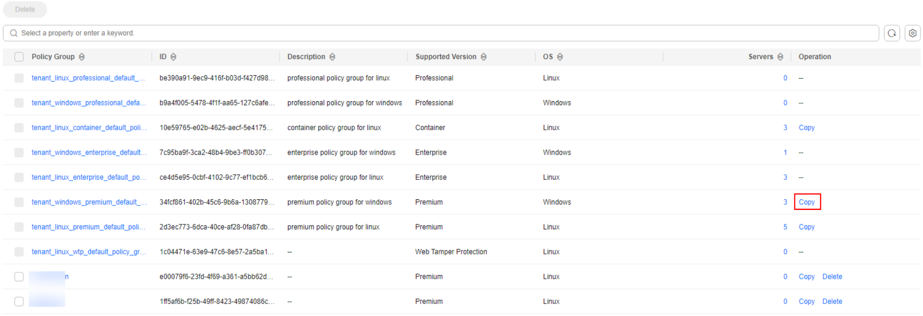
Delete

Select a property or enter a keyword.

Policy Group	ID	Description	Supported Version	OS	Servers	Operation
tenant_linux_professional_default_...	be390a91-9ec9-416f-b03d-f427d98...	professional policy group for linux	Professional	Linux	0	--
tenant_windows_professional_defa...	b9a4f005-5478-4f1f-aa65-127c6afe...	professional policy group for windows	Professional	Windows	0	--
tenant_linux_container_default_poli...	10e59765-e02b-4625-aecf-5e4175...	container policy group for linux	Container	Linux	3	Copy
tenant_windows_enterprise_default...	7c95ba9f-3ca2-48b4-9be3-ff0b307...	enterprise policy group for windows	Enterprise	Windows	1	--
tenant_linux_enterprise_default_po...	ce4d5e95-0cbf-4102-9c77-ef1bcb6...	enterprise policy group for linux	Enterprise	Linux	3	--
tenant_windows_premium_default_...	34fcf861-402b-45c6-9b6a-1308779...	premium policy group for windows	Premium	Windows	3	Copy
tenant_linux_premium_default_poli...	2d3ec773-6dca-40ce-af28-0fa87db...	premium policy group for linux	Premium	Linux	4	Copy
tenant_linux_wtp_default_policy_gr...	1c04471e-63e9-47c6-8e57-2a5ba1...	--	Web Tamper Protection	Linux	0	--
[redacted]	e00079f6-23fd-4f69-a361-a5bb62d...	--	Premium	Linux	0	Copy Delete
[redacted]	1ff5af6b-f25b-49ff-8423-49874086c...	--	Premium	Linux	0	Copy Delete

- Select the **tenant_windows_premium_default_policy_group** policy group. Click **Copy** in the **Operation** column.

Figure 3-10 Copying a Windows policy group



Policy Group	ID	Description	Supported Version	OS	Servers	Operation
tenant_linux_professional_default_...	be390a91-9ec9-416f-b03d-f427d98...	professional policy group for linux	Professional	Linux	0	--
tenant_windows_professional_defa...	b9a4f005-5478-4f1f-aa65-127c6afe...	professional policy group for windows	Professional	Windows	0	--
tenant_linux_container_default_poli...	10e59765-e02b-4625-aecf-5e4175...	container policy group for linux	Container	Linux	3	Copy
tenant_windows_enterprise_default...	7c95ba9f-3ca2-48b4-9be3-ff0b307...	enterprise policy group for windows	Enterprise	Windows	1	--
tenant_linux_enterprise_default_po...	ce4d5e95-0cbf-4102-9c77-ef1bcb6...	enterprise policy group for linux	Enterprise	Linux	3	--
tenant_windows_premium_default_...	34fcf861-402b-45c6-9b6a-1308779...	premium policy group for windows	Premium	Windows	3	Copy
tenant_linux_premium_default_poli...	2d3ec773-6dca-40ce-af28-0fa87db...	premium policy group for linux	Premium	Linux	5	Copy
tenant_linux_wtp_default_policy_gr...	1c04471e-63e9-47c6-8e57-2a5ba1...	--	Web Tamper Protection	Linux	0	--
[redacted]	e00079f6-23fd-4f69-a361-a5bb62d...	--	Premium	Linux	0	Copy Delete
[redacted]	1ff5af6b-f25b-49ff-8423-49874086c...	--	Premium	Linux	0	Copy Delete

Step 5 In the dialog box displayed, enter a policy group name and description, and click **OK**.

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.

Step 6 Click **OK**.

Step 7 Click the name of the policy group you just created. The policies in the group will be displayed.

Step 8 Click a policy name and modify its settings as required. For details, see **Configuring Policies**.

Step 9 Enable or disable the policy by clicking the corresponding button in the **Operation** column. You can click ⟳ to refresh the page.

----End

Applying a Policy Group

Step 1 Log in to the management console and go to the HSS page.

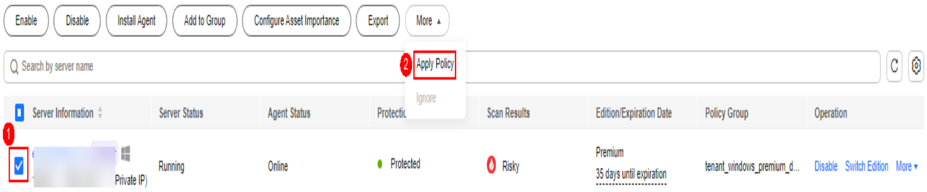
Step 2 In the navigation pane, choose **Asset Management** > **Servers & Quota** and click **Servers**.

Step 3 Select one or more servers for which you want to deploy a policy, and click **More** > **Apply Policy**.

NOTE

After protection is enabled for a server, the protection policy of the corresponding protection edition is deployed by default. For servers that use the premium and container editions, you can create and deploy different protection policies.

Figure 3-11 Applying a policy



☑ Server Information	Server Status	Agent Status	Protectic	Scan Results	Edition/Expiration Date	Policy Group	Operation
☑ [redacted] Private IP)	Running	Online	● Protected	Risky	Premium 35 days until expiration	tenant_windows_premium_d...	Disable Switch Edition More ▾

Step 4 In the dialog box that is displayed, select a policy group and click **OK**.

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

3.4.6 Managing Server Groups

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.

Creating a Server Group

After creating a server group, you can add servers to the group for unified management.

Step 1 Log in to the management console.

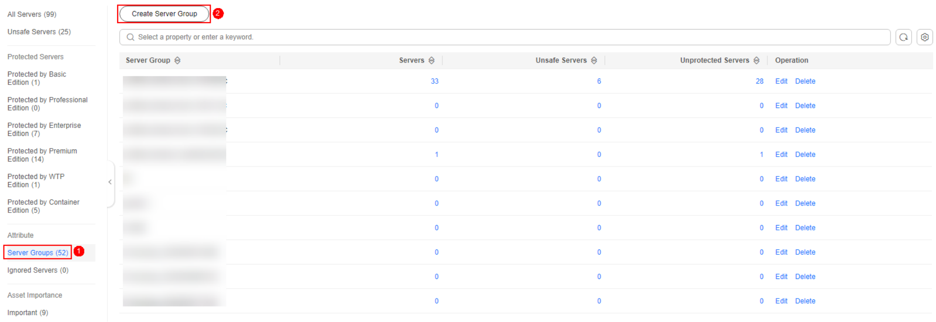
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**, click **Server Groups** in the **Server** list, and click **Create Server Group**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 3-12 Accessing the page of server groups


All Servers (99)
Unsafe Servers (25)
Protected Servers
Protected by Basic Edition (1)
Protected by Professional Edition (0)
Protected by Enterprise Edition (7)
Protected by Premium Edition (14)
Protected by WTP Edition (1)
Protected by Container Edition (5)
Attribute
Server Groups (52)
1
Ignored Servers (0)
Asset Importance
Important (9)
Create Server Group
2
Select a property or enter a keyword.

Server Group	Servers	Unsafe Servers	Unprotected Servers	Operation
[redacted]	33	6	28	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	1	0	1	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete

Step 4 In the **Create Server Group** dialog box, enter a server group name and select the servers to be added to the group.

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.

Step 5 Click **OK**.

----End

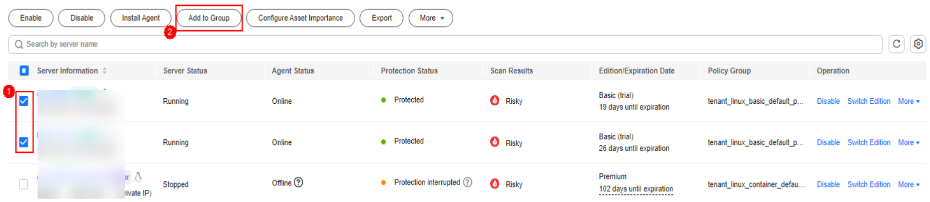
Adding Servers to Groups

You can add servers to an existing server group.

Step 1 Click the **Server** tab.

Step 2 Select one or more servers and click **Add to Group**.

Figure 3-13 Adding servers to a group



☐ Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Policy Group	Operation
☑ [redacted]	Running	Online	● Protected	Risky	Basic (trial) 19 days until expiration	tenant_linux_basic_default_p...	Disable Switch Edition More ▾
☑ [redacted]	Running	Online	● Protected	Risky	Basic (trial) 26 days until expiration	tenant_linux_basic_default_p...	Disable Switch Edition More ▾
☐ [redacted] rivate IP)	Stopped	Offline ?	● Protection interrupted ?	Risky	Premium 102 days until expiration	tenant_linux_container_defau...	Disable Switch Edition More ▾

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**.

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

Related Operations

Editing a server group

Step 1 Click **Servers & Quota** and click **Server Groups** on the **Servers** tab.

Step 2 Locate the row where a server group resides and click **Edit** in the **Operation** column.

Step 3 In the displayed dialog box, change the server group name and add or remove servers in the group.

Step 4 Click **OK**.

----End

Deleting a server group

Step 1 Click **Servers & Quota** and click **Server Groups** on the **Servers** tab.

Step 2 Locate the row where a server group resides and click **Delete** in the **Operation** column.

NOTE

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

----End

3.4.7 Servers Importance Management

By default, HSS considers all servers as general assets. You can configure the asset importance levels of servers and manage servers accordingly.

Assets are classified into the following types:

- **Important**. Specify this level for servers that run important services or store important data.
- **General**. Specify this level for servers that run general services or store general data.
- **Test**. Specify this level for servers that run test services or store test data.

Checking Asset Importance

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 In the lower part of the tab page, check the asset importance. You can click **Important**, **General**, or **Test** to view servers by importance level.

----End

Specifying Asset Importance

Step 1 Log in to the management console and go to the HSS page.

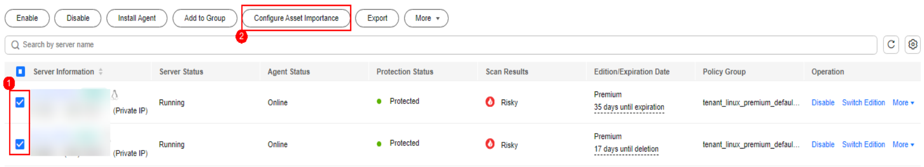
Step 2 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 3 Select the target servers and click **Configure Asset Importance** above the list.

Figure 3-14 Configure Asset Importance



Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Policy Group	Operation
☑ (Private IP)	Running	Online	● Protected	Risky	Premium 35 days until expiration	tenant_linux_premium_defaul...	Disable Switch Edition More
☑ (Private IP)	Running	Online	● Protected	Risky	Premium 17 days until deletion	tenant_linux_premium_defaul...	Disable Switch Edition More

Step 4 In the dialog box that is displayed, select an asset importance level.

Step 5 Confirm the information and click **OK**.

----End

3.4.8 Ignoring a Server

You can ignore the servers that do not need to be protected. HSS will neither protect the ignored servers nor synchronize the information changes of the ignored servers.

Prerequisite

You do not enable protection for the target server.

Ignoring a 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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**.

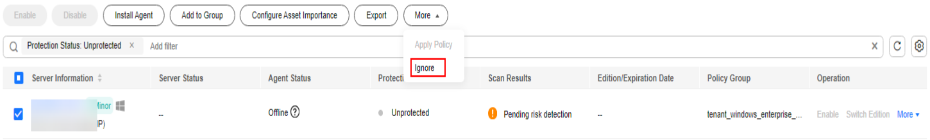
NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the **Servers** tab.

Step 5 Select the target server and click **More** > **Ignore** above the server list to ignore the server.

Figure 3-15 Ignoring a server



Server Information	Server Status	Agent Status	Protecti	Scan Results	Edition/Expiration Date	Policy Group	Operation
☑ Minor P)	--	Offline	Unprotected	Pending risk detection	--	tenant_windows_enterprise_...	Enable Switch Edition More

----End

Unignoring a 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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**.

NOTE

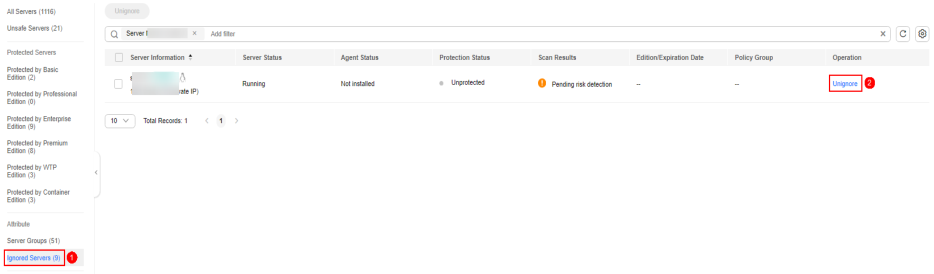
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the **Servers** tab.

Step 5 In the **Attribute** area, choose **Ignored Servers** to view the list of ignored servers.

Step 6 In the row of the target server, click **Unignore** in the **Operation** column.

Figure 3-16 Unignoring a server


All Servers (1116)
Unsafe Servers (21)
Protected Servers
Protected by Basic Edition (2)
Protected by Professional Edition (0)
Protected by Enterprise Edition (9)
Protected by Premium Edition (8)
Protected by WTP Edition (3)
Protected by Container Edition (3)
Attribute
Server Groups (51)
Ignored Servers (9)
1
Unignore
Server I [redacted]
Add filter
2

Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Policy Group	Operation
[redacted] ate IP)	Running	Not installed	Unprotected	Pending risk detection	--	--	Unignore

10 Total Records: 1 < 1 >

----End

3.5 Container Management

3.5.1 Viewing the Container Node Protection Status

The **Container Nodes** page displays the protection, node, and Agent status of clusters in Cloud Container Engine (CCE), helping you learn the security status of clusters in real time.

Constraints

- Only Linux servers are supported.
- Servers that are not protected by HSS enterprise, premium, WTP, or container editions cannot perform container-related operations.

Viewing the Clusters and Protection 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Containers & Quota**. Click **Container Nodes**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 View the node protection status. You can obtain the details in **Table 3-11**.

NOTE

In the HSS container node list, you can view only the servers where the agent has been installed. To view the servers where the agent has not been installed, choose **Asset Management** > **Servers & Quota**.

Table 3-11 Parameter description

Parameter	Description
Server Information	Server name and IP address. Move the cursor over to the server name to view the server details, including the server ID, OS, system name, and system version.
Protection Status	Protection status of a node. The options are as follows: ● **Unprotected**: HSS is disabled for the server. After the agent is installed, click **Enable** in the **Operation** column to enable protection. ● **Enabled**: The server is fully protected by HSS. ● **Protection interrupted**: The server is shut down, the agent is offline, or the agent is uninstalled.
Server Status	● Running ● Unavailable ● Normal
Agent Status	You can select a status to view the server. ● **Online**: The agent is running properly. ● **Offline**: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers. **NOTE** The server information will be automatically deleted from the node management page after the agent goes offline for 30 days. ● **Not installed**: The agent has not been installed or successfully started.

----End

3.5.2 Exporting the Container Node List

This section describes how to export the container node list to your local PC.

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Choose the **Container Nodes** tab.

Step 5 In the upper part of the container list, click **Export** to export the list.

You can select multiple container nodes and click **Export** to export their container details in batches.

NOTE

The information about up to 1,000 container nodes can be exported at a time.

----End

3.5.3 Disabling Protection for Container Edition

You can disable the container edition for a server. A quota that has been unbound from a server can be bound to another one.

Before You Start

- Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.
- To unsubscribe from the pay-per-use quota of the container edition, you just need to disable the protection.

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 In the **Operation** column of a server, click **Disable Protection**.

To disable protection in batches, select multiple target servers and click **Disable Protection**.

Step 5 In the dialog box that is displayed, confirm the information and click **OK**.

Step 6 Choose **Asset Management** > **Containers & Quota** and click the **Container Nodes** tab. Check the container protection status in the server list. If it is **Unprotected**, the protection has been disabled.

⚠ CAUTION

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

----End

3.5.4 Container Images

3.5.4.1 Local Images

You can manually scan local images for vulnerabilities and software information and provides scan reports. This section describes how to perform security scans on local images and view scan reports.

Constraints

- Only the HSS container edition supports this function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- Only the local images of the Docker engine can be reported to the HSS console.
- Security scans can be performed only on Linux images.

Viewing Local Images

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the **Container Images** tab and click **Local image**.

You can view the name, version, type, and security risks of an image.

- Viewing information about servers associated with an image

  Locate the row that contains the target image and click the server name. The associated servers page is displayed. You can view details about the servers associated with the image.

- Viewing information about containers associated with an image

  Locate the row that contains the target image and click the number in the **Associated Containers** column. The **Associated Containers** page is displayed. You can view details about the containers associated with the image.

- Viewing information about image components

  Locate the row that contains the target image and click the number in the **Components** column. The **Components** page is displayed. You can view details about image components.

- Viewing image security risks

  You can view the number of risky images and click the value to go to the risk details page.

----End

Local Image Security Scans

You can choose all images, multiple images, or a single image and manually start a scan. The duration of a security scan depends on the scanned image size. Generally, scanning an image takes shorter than 3 minutes. After the scan is complete, click **View Report** to check the report.

The following security scan items are supported for local images:

Scan Item	Description
Vulnerability	Detects vulnerabilities in images.
Installed software	Collects software information in an image.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **Local image**.

Step 4 Performs a security scan for a single image or multiple images.

- Single image security scan

  In the **Operation** column of the target image, click **Scan** to perform security scan.

- Batch image security scan

  Select all target images and click **Scan** above the image list to perform security scan for multiple target images.

- Full image security scan

  Click **Scan All** above the image list to perform a security scan for all images.

NOTICE

A full scan takes a long time and cannot be interrupted after it starts. Exercise caution when performing this operation.

Step 5 In the displayed dialog box, click **OK** to start the scan job.

After a full scan task is started, you can move the cursor over the gray **Scan All** button to view the scan progress.

Step 6 The image security scan is complete, when the **Scan Status** changes to **Completed** and the **Latest Scan Completed** shows the latest task execution time.

----End

Viewing Local Image Vulnerability Reports and Software Information

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 3 Click the **Container Images** tab and click **Local image**.

Step 4 In the **Operation** column of the target image, click **View Report**. On the displayed page, view vulnerability reports and software information.

----End

Exporting Local Image Vulnerability Reports

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **Local image**.

Step 4 Click **Export Vulnerability** above the image list.

If you want to export the vulnerability report of a specified image, select the image type in the search box and click **Export Vulnerability**.

Step 5 View the export status in the upper part of the container management page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

3.5.4.2 Managing SWR Private Images

Images in the private image repository come from SWR images. You can manually scan for and check reports on software compliance, base image information, vulnerabilities, malicious files, software information, file information, baseline check, sensitive information.

Constraints

- Only the HSS container edition supports this function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- Security scans can be performed only on Linux images.

Viewing Private Images

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Container Images** tab and click **SWR private image**.

Step 5 You can click **Update Private Images from SWR** to update self-owned images from SWR.

NOTE

Images can be synchronized only after being authorized by SWR. For details, see **SWR Authorization Methods**.

----End

Scanning a Private Image

You can choose all images, multiple images, or a single image and manually start a scan. The duration of a security scan depends on the scanned image size. Generally, scanning an image takes shorter than 3 minutes. After the scan is complete, click **View Report** to check the report.

Scan items of private images in SWR are as follows:

Scan Item	Description
Vulnerability	Detect system and application vulnerabilities in images.
Malicious file	Detects malicious files in images.
Software information	Collects software information in an image.

Scan Item	Description
File information	Collects file information in an image.
Unsafe setting	● Configuration check: – Checks the images configurations of CentOS 7, Debian 10, EulerOS, and Ubuntu16. – Checks SSH configurations. ● Weak password check: detects weak passwords in images. ● Password complexity check: detects insecure password complexity policies in images.
Sensitive information	Detects files that contain sensitive information in images. ● The paths that are not checked by default are as follows: – /usr/* – /lib/* – /lib32/* – /bin/* – /sbin/* – /var/lib/* – /var/log/* – *Any path*/node_modules/*any path*/*any name*.md – *Any path*/node_modules/*any path*/test/*any path* – */service/iam/examples_test.go – *Any path*/grafana/public/build/*any name*.js **NOTE** ● Any path: indicates that the current path is a customized value and can be any path in the system. ● Any name: indicates that the file name in the current path is a customized value, which can be any name ended with .md or .js in the system. ● On the **View Report** > **Sensitive Information** tab, click **Configure Sensitive File Path** to set the Linux path of the file that does not need to be checked. A maximum of 20 paths can be added. ● No checks are performed in the following scenarios: – The file size is greater than 20 MB. – The file type can be binary, common process, or auto generation.
Software compliance	Detects software and tools that are not allowed to be used.
Basic image information	Detects service images that are not created using base images.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR private image**.

Step 4 Perform a security scan for a single image or multiple images.

NOTE

- Multi-architecture images do not support batch scan or full scan.
- A full scan takes a long time and cannot be interrupted after it starts. Exercise caution when performing this operation.

- Single image security scan

  In the **Operation** column of the target image, click **Scan** to perform security scan.

- Batch image security scan

  Select all target images and click **Scan** above the image list to perform security scan for multiple target images.

- Full image security scan

  Click **Scan All** above the image list to perform a security scan for all images.

Step 5 In the displayed dialog box, click **OK** to start the scan job.

After a full scan task is started, you can move the cursor over the grey **Scan All** button to view the scan progress.

Step 6 **Scanned** in the **Scan Status** column indicates the target image scan completed.

----End

Checking the Vulnerability Report of Private Images

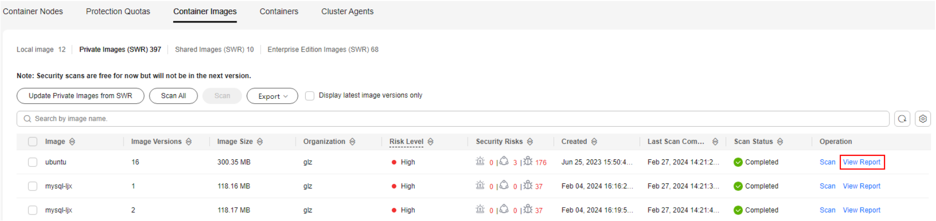
After the scanning is complete, you can view the security reports.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and select **SWR private image**. Click **Security Report** in the **Operation** column to view the report details of the image version.

Figure 3-17 Security report



Note: Security scans are free for now but will not be in the next version.

Image	Image Versions	Image Size	Organization	Risk Level	Security Risks	Created	Last Scan Com...	Scan Status	Operation
ubuntu	16	300.35 MB	glz	High	0 | 3 | 176	Jun 25, 2023 15:50:4...	Feb 27, 2024 14:21:2...	Completed	Scan View Report
mysql-ljx	1	118.16 MB	glz	High	0 | 0 | 37	Feb 04, 2024 16:16:2...	Feb 27, 2024 14:21:3...	Completed	Scan View Report
mysql-ljx	2	118.17 MB	glz	High	0 | 0 | 37	Feb 04, 2024 16:19:5...	Feb 27, 2024 14:21:4...	Completed	Scan View Report

Step 4 Choose **Vulnerability Reports** to view the vulnerability report.

- Viewing vulnerability details

  Click the vulnerability name to go to the vulnerability details page and view the basic information and affected images.

- Viewing the **CVE ID**, **CVSS Score**, and **Disclosed Time** of a vulnerability

  Click ˅ in front of the target vulnerability name to view the **CVE ID**, **CVSS Score**, and **Disclosed Time**.

- Viewing vulnerability solutions

  In the **Solution** column of the row containing the target vulnerability, click the solution description to view the vulnerability solution details.

----End

Viewing the Malicious File Report of a Private Image

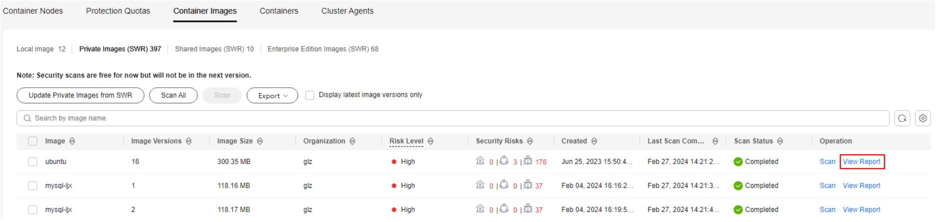
After images are scanned, you can view malicious files on them. This section describes how to view malicious files in an image version.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and select **SWR private image**. Click **Security Report** in the **Operation** column to view the report details of the image version.

Figure 3-18 Security report



Note: Security scans are free for now but will not be in the next version.

	Image	Image Versions	Image Size	Organization	Risk Level	Security Risks	Created	Last Scan Com...	Scan Status	Operation
□	ubuntu	16	300.35 MB	glz	● High	0 | 3 | 176	Jun 25, 2023 15:50:4...	Feb 27, 2024 14:21:2...	✓ Completed	Scan View Report
□	mysql-ljx	1	118.16 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:16:2...	Feb 27, 2024 14:21:3...	✓ Completed	Scan View Report
□	mysql-ljx	2	118.17 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:19:5...	Feb 27, 2024 14:21:4...	✓ Completed	Scan View Report

Step 4 Click **Malicious Files** to view malicious files on the image.

----End

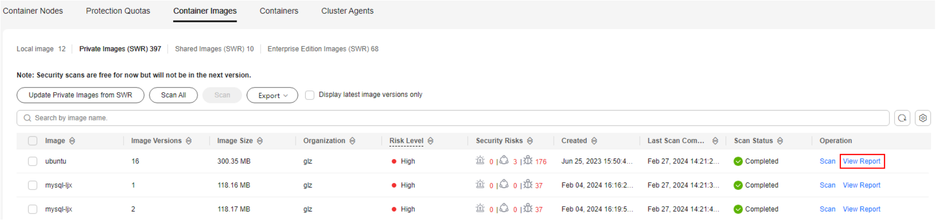
Viewing Software Information About a Private Image

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and select **SWR private image**. Click **Security Report** in the **Operation** column to view the report details of the image version.

Figure 3-19 Security report



Note: Security scans are free for now but will not be in the next version.

	Image	Image Versions	Image Size	Organization	Risk Level	Security Risks	Created	Last Scan Com...	Scan Status	Operation
□	ubuntu	16	300.35 MB	glz	● High	0 | 3 | 176	Jun 25, 2023 15:50:4...	Feb 27, 2024 14:21:2...	✓ Completed	Scan View Report
□	mysql-ljx	1	118.16 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:16:2...	Feb 27, 2024 14:21:3...	✓ Completed	Scan View Report
□	mysql-ljx	2	118.17 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:19:5...	Feb 27, 2024 14:21:4...	✓ Completed	Scan View Report

Step 4 Click **Software Information** to view the software contained in the image version, software type, and number of vulnerabilities in the software.

Step 5 Click ﹀ next to a software name to view the software vulnerability name, repair urgency, and solution.

----End

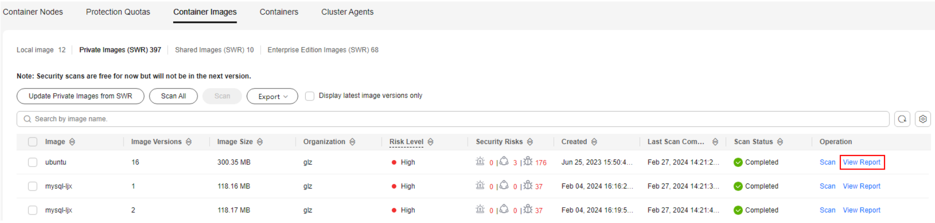
Viewing File Information About a Private Image

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and select **SWR private image**. Click **Security Report** in the **Operation** column to view the report details of the image version.

Figure 3-20 Security report



Note: Security scans are free for now but will not be in the next version.

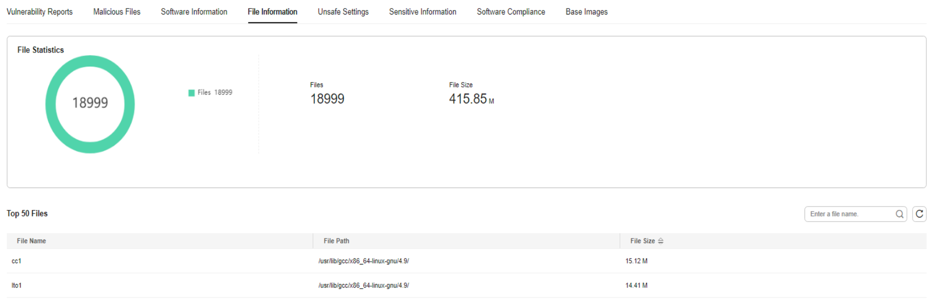
Update Private Images from SWR
Scan All
Scan
Export
□ Display latest image versions only
Search by image name.

	Image	Image Versions	Image Size	Organization	Risk Level	Security Risks	Created	Last Scan Com...	Scan Status	Operation
□	ubuntu	16	300.35 MB	glz	● High	0 | 3 | 176	Jun 25, 2023 15:50:4...	Feb 27, 2024 14:21:2...	✓ Completed	Scan View Report
□	mysql-ljx	1	118.16 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:16:2...	Feb 27, 2024 14:21:3...	✓ Completed	Scan View Report
□	mysql-ljx	2	118.17 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:19:5...	Feb 27, 2024 14:21:4...	✓ Completed	Scan View Report

Step 4 Click **File Information** to view the file information about the image.

Including the number of files, total file size, and details about the top 50 files.

Figure 3-21 File information



Files
18999

File Size
415.85 M

Top 50 Files

File Name	File Path	File Size
cc1	/usr/lib/gcc/x86_64-linux-gnu/4.9/	15.12 M
lto1	/usr/lib/gcc/x86_64-linux-gnu/4.9/	14.41 M

----End

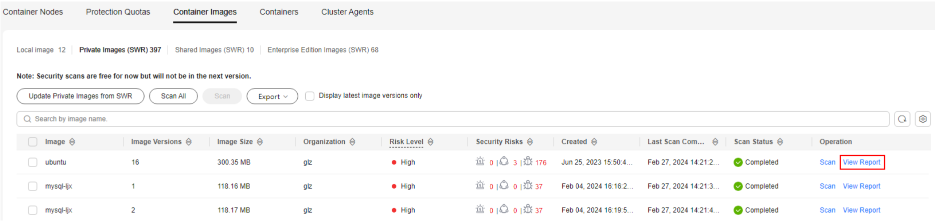
Viewing the Unsafe Settings of a Private Image

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and select **SWR private image**. Click **Security Report** in the **Operation** column to view the report details of the image version.

Figure 3-22 Security report



Note: Security scans are free for now but will not be in the next version.

Update Private Images from SWR
Scan All
Scan
Export
□ Display latest image versions only
Search by image name.

	Image	Image Versions	Image Size	Organization	Risk Level	Security Risks	Created	Last Scan Com...	Scan Status	Operation
□	ubuntu	16	300.35 MB	glz	● High	0 | 3 | 176	Jun 25, 2023 15:50:4...	Feb 27, 2024 14:21:2...	✓ Completed	Scan View Report
□	mysql-ljx	1	118.16 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:16:2...	Feb 27, 2024 14:21:3...	✓ Completed	Scan View Report
□	mysql-ljx	2	118.17 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:19:5...	Feb 27, 2024 14:21:4...	✓ Completed	Scan View Report

Step 4 Select **Unsafe Settings** to view the baseline check report.

You can view the unsafe configurations, password complexity policy detection, and common weak password detection results of the target image.

- Viewing unsafe configurations and modification suggestions
  a. On the **Unsafe Configurations** tab page, select the target baseline.
  b. In the detection item column of the target detection item, click **Description** to view the detection item description and modification suggestions.
- Common weak password detection
  a. Click **Common Weak Password Detection**.
  b. Configure weak passwords and click **OK**.

----End

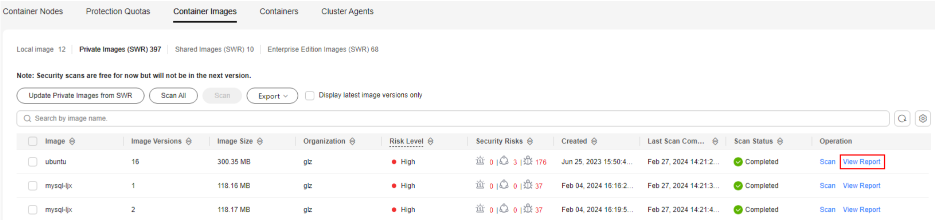
Viewing the Sensitive Information Report of a Private Image

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and select **SWR private image**. Click **Security Report** in the **Operation** column to view the report details of the image version.

Figure 3-23 Security report



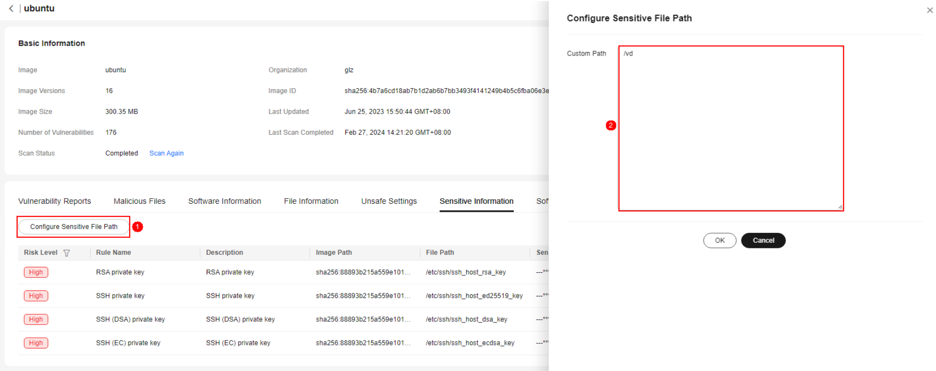
Note: Security scans are free for now but will not be in the next version.

Image	Image Versions	Image Size	Organization	Risk Level	Security Risks	Created	Last Scan Com...	Scan Status	Operation
ubuntu	16	300.35 MB	glz	● High	0 | 3 | 176	Jun 25, 2023 15:50:4...	Feb 27, 2024 14:21:2...	Completed	Scan View Report
mysql-ljx	1	118.16 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:16:2...	Feb 27, 2024 14:21:3...	Completed	Scan View Report
mysql-ljx	2	118.17 MB	glz	● High	0 | 0 | 37	Feb 04, 2024 16:19:5...	Feb 27, 2024 14:21:4...	Completed	Scan View Report

Step 4 Click the **Sensitive Information** tab to view details about sensitive image information and ignore risk alarms.

Step 5 Click **Configure Sensitive File Path** to view and edit the custom file path whitelist.

Figure 3-24 Editing the sensitive file whitelist



Basic Information

Image	ubuntu	Organization	glz
Image Versions	16	Image ID	sha256:4b7a6cd18ab7b1d2ab6b7bb3493f4141249b4b5c6fba06e3e
Image Size	300.35 MB	Last Updated	Jun 25, 2023 15:50:44 GMT+08:00
Number of Vulnerabilities	176	Last Scan Completed	Feb 27, 2024 14:21:20 GMT+08:00
Scan Status	Completed Scan Again		

Risk Level	Rule Name	Description	Image Path	File Path	Sen
High	RSA private key	RSA private key	sha256:88893b215a559e101...	/etc/ssh/ssh_host_rsa_key	---**
High	SSH private key	SSH private key	sha256:88893b215a559e101...	/etc/ssh/ssh_host_ed25519_key	---**
High	SSH (DSA) private key	SSH (DSA) private key	sha256:88893b215a559e101...	/etc/ssh/ssh_host_dsa_key	---**
High	SSH (EC) private key	SSH (EC) private key	sha256:88893b215a559e101...	/etc/ssh/ssh_host_ecdsa_key	---**

Custom Path: /vd

Table 3-12 Custom path description

Path Specification Item	Description	Example Value
OS	Only Linux is supported.	-
Requirement	A maximum of 20 paths can be specified. One path occupies one line.	/usr/ /lib/test.txt
Default whitelist path	The following whitelist directories or file formats are supported by default and do not need to be configured: ● /usr/* ● /lib/* ● /lib32/* ● /bin/* ● /sbin/* ● /var/lib/* ● /var/log/* ● *Any path*/node_modules/*any path*/*any name*.md ● *Any path*/node_modules/*any path*/test/*any path* ● */service/iam/examples_test.go ● *Any path*/grafana/public/build/*any name*.js **NOTE** ● Any path: indicates that the current path is a customized value and can be any path in the system. ● Any name: indicates that the file name in the current path is a customized value, which can be any name ended with .md or .js in the system.	-
Non-scanning scenario	● The file size is greater than 20 MB. ● The following file types are not scanned: – Common binary files – Common program files – Automatically generated files	● jpg|png|gif|mov|avi|mpeg|pdf|mp4|mp3|svg|tar|gz|zip ● js|jar|java||md|cpp|cxx|scala|pl ● [0-9a-zA-Z_-]{32,64}

----End

Viewing the Software Compliance Report About a Private Image

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR private image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **Software Compliance** to view the report.

You can view the name, software version, path, and image layer of non-compliant software.

----End

Viewing the Base Image Report of a Private Image

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR private image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Click the **Base Images** tab and view reports.

You can view the name, version, and image layer path of a service image that is not created using a base image.

----End

Exporting a Private Image Vulnerability Report or Baseline Report

NOTE

Vulnerability or baseline report cannot be exported for multi-architecture images.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR private image**.

Step 4 Click **Export Vulnerability** above the image list and select a report type to export the vulnerability or baseline report.

If you want to export the vulnerability report of a specified image, select the image type in the search box and click **Export Vulnerability**.

Step 5 View the export status in the upper part of the container management page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

3.5.4.3 Managing SWR Shared Images

You can manually scan for and check reports on software compliance, base image information, vulnerabilities, malicious files, software information, file information, baseline check, sensitive information. This section describes how to perform security scans on SWR shared images and view scan reports.

Constraints

- Only the HSS container edition supports this function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- Security scans can be performed only on Linux images.

Viewing SWR Shared Images

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

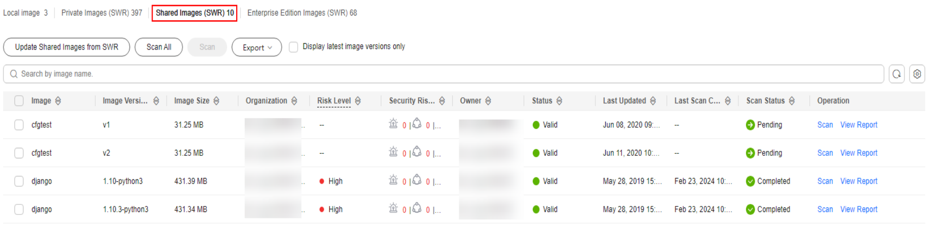
NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Container Images** tab and click **SWR shared image** to view the shared image list.

You can view the version, size, organization, security risks, and owner of a shared image.

Figure 3-25 Viewing shared images



□	Image	Image Versi...	Image Size	Organization	Risk Level	Security Ris...	Owner	Status	Last Updated	Last Scan C...	Scan Status	Operation
□	cfgtest	v1	31.25 MB	[redacted]	--	0 | 0 |...	[redacted]	● Valid	Jun 08, 2020 09:...	--	Pending	Scan View Report
□	cfgtest	v2	31.25 MB	[redacted]	--	0 | 0 |...	[redacted]	● Valid	Jun 11, 2020 10:...	--	Pending	Scan View Report
□	django	1.10-python3	431.39 MB	[redacted]	● High	0 | 0 |...	[redacted]	● Valid	May 28, 2019 15:...	Feb 23, 2024 10:...	✓ Completed	Scan View Report
□	django	1.10.3-python3	431.34 MB	[redacted]	● High	0 | 0 |...	[redacted]	● Valid	May 28, 2019 15:...	Feb 23, 2024 10:...	✓ Completed	Scan View Report

- Updating a shared image

  Click **Update Shared Images from SWR** to update the shared image list.

- Filtering images of the latest version

  If you select **Display latest image versions only**, you can filter the latest images of all images.

----End

Shared Image Security Scan

You can manually scan an SWR shared image in **Valid** state. The scan items are as follows:

Scan Item	Description
Vulnerability	Detect system and application vulnerabilities in images.
Malicious file	Detects malicious files in images.
Software information	Collects software information in an image.
File information	Collects file information in an image.
Unsafe setting	● Configuration check: – Checks the images configurations of CentOS 7, Debian 10, EulerOS, and Ubuntu16. – Checks SSH configurations. ● Weak password check: detects weak passwords in images. ● Password complexity check: detects insecure password complexity policies in images.

Scan Item	Description
Sensitive information	Detects files that contain sensitive information in images. ● The paths that are not checked by default are as follows: – /usr/* – /lib/* – /lib32/* – /bin/* – /sbin/* – /var/lib/* – /var/log/* – *Any path*/node_modules/*any path*/*any name*.md – *Any path*/node_modules/*any path*/test/*any path* – */service/iam/examples_test.go – *Any path*/grafana/public/build/*any name*.js NOTE ● Any path: indicates that the current path is a customized value and can be any path in the system. ● Any name: indicates that the file name in the current path is a customized value, which can be any name ended with .md or .js in the system. ● On the **View Report** > **Sensitive Information** tab, click **Configure Sensitive File Path** to set the Linux path of the file that does not need to be checked. A maximum of 20 paths can be added. ● No checks are performed in the following scenarios: – The file size is greater than 20 MB. – The file type can be binary, common process, or auto generation.
Software compliance	Detects software and tools that are not allowed to be used.
Basic image information	Detects service images that are not created using base images.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 Performs a security scan for a single image or multiple images.

NOTE

- You can perform a security scan only when the status is **Valid**.
- Multi-architecture images do not support batch scan or full scan.
- A full scan takes a long time and cannot be interrupted after it starts. Exercise caution when performing this operation.

- Single image security scan

  In the **Operation** column of the target image, click **Scan** to perform security scan.
- Batch image security scan

  Select all target images and click **Scan** above the image list to perform security scan for multiple target images.
- Full image security scan

  Click **Scan All** above the image list to perform a security scan for all images.

Step 5 In the displayed dialog box, click **OK** to start the scan job.

After a full scan task is started, you can move the cursor over the grey **Scan All** button to view the scan progress.

Step 6 The image security scan is complete, when the **Scan Status** changes to **Completed** and the **Latest Scan Completed** shows the latest task execution time.

----End

Viewing the SWR Shared Image Vulnerability Scan Report

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **Vulnerability Reports** to view the vulnerability report.

- Viewing vulnerability details

  Click the vulnerability name to go to the vulnerability details page and view the basic information and affected images.
- Viewing the **CVE ID**, **CVSS Score**, and **Disclosed Time** of a vulnerability

  Click ⌄ in front of the target vulnerability name to view the **CVE ID**, **CVSS Score**, and **Disclosed Time**.
- Viewing vulnerability solutions

  In the **Solution** column of the row containing the target vulnerability, click the solution description to view the vulnerability solution details.

----End

Viewing the Malicious Files Report of SWR Shared Images

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Select **Malicious Files** to view the malicious files report.

You can view the name, path, size, and description of the malicious file in the target image.

----End

Viewing the SWR Shared Image Software Information Report

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **Software Information** to view the report.

You can view the software name, type, version, and number of vulnerabilities in the image.

----End

Viewing the SWR Shared Image File Information Report

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **File Information** to view the report.

You can view the number of files in the target image, total file size, and details about the top 50 files in size.

----End

Viewing the SWR Shared Image Baseline Check Report

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Select **Unsafe Settings** to view the baseline check report.

You can view the unsafe configurations, password complexity policy detection, and common weak password detection results of the target image.

- Viewing unsafe configurations and modification suggestions
  a. On the **Unsafe Configurations** tab page, select the target baseline.
  b. In the detection item column of the target detection item, click **Description** to view the detection item description and modification suggestions.
- Common weak password detection
  a. Click **Common Weak Password Detection**.
  b. Configure weak passwords and click **OK**.

----End

Viewing the SWR Shared Image Sensitive Information Report

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Click the **Sensitive Information** tab to view the report.

You can view the path, sensitive information, and risk level of the file that contains sensitive information in the target image.

- Prompt for ignoring sensitive information

  In the **Operation** column of the target sensitive information file, click **Ignore** to ignore the sensitive information that you think is secure.
- Configuring the sensitive file path
  a. Click **Configure Sensitive File Path**. The file path management page is displayed on the right.
  b. In the dialog box that is displayed, set the Linux path of the file that does not need to be checked and click **OK**.

     A maximum of 20 paths can be specified. One path occupies one line.

----End

Viewing the SWR Shared Image Software Compliance Report

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **Software Compliance** to view the report.

You can view the name, software version, path, and image layer of non-compliant software.

----End

Viewing the SWR Shared Image Base Images Information Report

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **Base Images** to view the report.

You can view the name, version, and image layer path of a service image that is not created using a base image.

----End

Exporting the SWR Shared Image Vulnerability or Baseline Report

NOTE

Vulnerability reports cannot be exported for multi-architecture images.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 Click **Export Vulnerability** above the image list and select a report type to export the vulnerability or baseline report.

If you want to export the vulnerability report of a specified image, select the image type in the search box and click **Export Vulnerability**.

Step 5 View the export status in the upper part of the container management page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

3.5.4.4 SWR Enterprise Edition Image

You can manually scan for and check reports on software compliance, base image information, vulnerabilities, malicious files, software information, file information, baseline check, sensitive information. This section describes how to perform security scans on SWR enterprise images and view scan reports.

Constraints

- Only the HSS container edition supports this function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- Security scans can be performed only on Linux images.

Viewing SWR Enterprise Edition Images

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** > **HSS**.

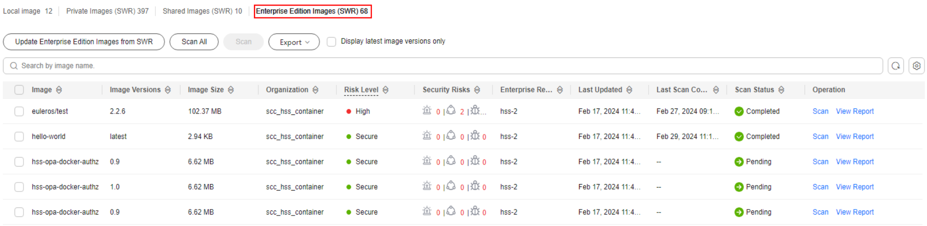
Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

> NOTE
>
> If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

You can view the version, size, organization, security risks, and owner of an enterprise image.

Figure 3-26 Viewing an image of the enterprise edition


Local image 12
Private Images (SWR) 397
Shared Images (SWR) 10
Enterprise Edition Images (SWR) 68
Update Enterprise Edition Images from SWR
Scan All
Scan
Export
Display latest image versions only
Search by image name.

□	Image	Image Versions	Image Size	Organization	Risk Level	Security Risks	Enterprise Re...	Last Updated	Last Scan Co...	Scan Status	Operation
□	euleros/test	2.2.6	102.37 MB	scc_hss_container	● High	0 | 2 | ...	hss-2	Feb 17, 2024 11:4...	Feb 27, 2024 09:1...	Completed	Scan View Report
□	hello-world	latest	2.94 KB	scc_hss_container	● Secure	0 | 0 | 0	hss-2	Feb 17, 2024 11:4...	Feb 29, 2024 11:1...	Completed	Scan View Report
□	hss-opa-docker-authz	0.9	6.62 MB	scc_hss_container	● Secure	0 | 0 | 0	hss-2	Feb 17, 2024 11:4...	--	Pending	Scan View Report
□	hss-opa-docker-authz	1.0	6.62 MB	scc_hss_container	● Secure	0 | 0 | 0	hss-2	Feb 17, 2024 11:4...	--	Pending	Scan View Report
□	hss-opa-docker-authz	0.9	6.62 MB	scc_hss_container	● Secure	0 | 0 | 0	hss-2	Feb 17, 2024 11:4...	--	Pending	Scan View Report

- Updating an image of the enterprise edition

  Click **Update Enterprise Edition Images from SWR**.
- Filtering images of the latest version

  If you select **Display latest image versions only**, you can filter the latest images of all images.

----End

Image Security Scanning for SWR Enterprise Edition

You can choose all images, multiple images, or a single image and manually start a scan. The duration of a security scan depends on the scanned image size.

Generally, scanning an image takes shorter than 3 minutes. After the scan is complete, click **View Report** to check the report.

SWR enterprise edition images support the following security scan items:

Scan Item	Description
Vulnerability	Detect system and application vulnerabilities in images.
Malicious file	Detects malicious files in images.
Software information	Collects software information in an image.
File information	Collects file information in an image.
Unsafe setting	● Configuration check: – Checks the images configurations of CentOS 7, Debian 10, EulerOS, and Ubuntu16. – Checks SSH configurations. ● Weak password check: detects weak passwords in images. ● Password complexity check: detects insecure password complexity policies in images.

Scan Item	Description
Sensitive information	Detects files that contain sensitive information in images. ● The paths that are not checked by default are as follows: – /usr/* – /lib/* – /lib32/* – /bin/* – /sbin/* – /var/lib/* – /var/log/* – *Any path*/node_modules/*any path*/*any name*.md – *Any path*/node_modules/*any path*/test/*any path* – */service/iam/examples_test.go – *Any path*/grafana/public/build/*any name*.js **NOTE** ● Any path: indicates that the current path is a customized value and can be any path in the system. ● Any name: indicates that the file name in the current path is a customized value, which can be any name ended with .md or .js in the system. ● On the **View Report** > **Sensitive Information** tab, click **Configure Sensitive File Path** to set the Linux path of the file that does not need to be checked. A maximum of 20 paths can be added. ● No checks are performed in the following scenarios: – The file size is greater than 20 MB. – The file type can be binary, common process, or auto generation.
Software compliance	Detects software and tools that are not allowed to be used.
Basic image information	Detects service images that are not created using base images.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

Step 4 Performs a security scan for a single image or multiple images.

NOTE

- Multi-architecture images do not support batch scan or full scan.
- A full scan takes a long time and cannot be interrupted after it starts. Exercise caution when performing this operation.

- Single image security scan

  In the **Operation** column of the target image, click **Scan** to perform security scan.
- Batch image security scan

  Select all target images and click **Scan** above the image list to perform security scan for multiple target images.
- Full image security scan

  Click **Scan All** above the image list to perform a security scan for all images.

Step 5 In the displayed dialog box, click **OK** to start the scan job.

After a full scan task is started, you can move the cursor over the dimmed **Scan All** button to view the scan progress.

Step 6 The image security scan is complete, when the **Scan Status** changes to **Completed** and the **Latest Scan Completed** shows the latest task execution time.

----End

Viewing the Vulnerability Scan Report of the Enterprise Edition Image (SWR)

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **Vulnerability Reports** to view the vulnerability report.

- Viewing vulnerability details

  Click the vulnerability name to go to the vulnerability details page and view the basic information and affected images.
- Viewing the **CVE ID**, **CVSS Score**, and **Disclosed Time** of a vulnerability

  Click ⌄ in front of the target vulnerability name to view the **CVE ID**, **CVSS Score**, and **Disclosed Time**.
- Viewing vulnerability solutions

  In the **Solution** column of the row containing the target vulnerability, click the solution description to view the vulnerability solution details.

----End

Viewing the Malicious Image File Report of SWR Enterprise Edition

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Select **Malicious Files** to view the malicious files report.

You can view the name, path, size, and description of the malicious file in the target image.

----End

Viewing the Image Software Information Report of SWR Enterprise Edition

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click the **Container Images** tab and click **SWR shared image**.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **Software Information** to view the report.

You can view the software name, type, version, and number of vulnerabilities in the image.

----End

Viewing the Image File Information Report of SWR Enterprise Edition

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **File Information** to view the report.

You can view the number of files in the target image, total file size, and details about the top 50 files in size.

----End

Viewing the Image Baseline Check Report of SWR Enterprise Edition

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Select **Unsafe Settings** to view the baseline check report.

You can view the unsafe configurations, password complexity policy detection, and common weak password detection results of the target image.

- Viewing unsafe configurations and modification suggestions
  a. On the **Unsafe Configurations** tab page, select the target baseline.
  b. In the detection item column of the target detection item, click **Description** to view the detection item description and modification suggestions.
- Common weak password detection
  a. Click **Common Weak Password Detection**.
  b. Configure weak passwords and click **OK**.

----End

Viewing the Image Sensitive Information Report of SWR Enterprise Edition

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Click the **Sensitive Information** tab to view the report.

You can view the path, sensitive information, and risk level of the file that contains sensitive information in the target image.

- Prompt for ignoring sensitive information

  In the **Operation** column of the target sensitive information file, click **Ignore** to ignore the sensitive information that you think is secure.
- Configuring the sensitive file path
  a. Click **Configure Sensitive File Path**. The file path management page is displayed on the right.
  b. In the dialog box that is displayed, set the Linux path of the file that does not need to be checked and click **OK**.

     A maximum of 20 paths can be specified. One path occupies one line.

----End

Viewing the Image Software Compliance Report of SWR Enterprise Edition

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Choose **Software Compliance** to view the report.

You can view the name, software version, path, and image layer of non-compliant software.

----End

Viewing the Basic Image Information Report of SWR Enterprise Edition

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

Step 4 In the **Operation** column of the target image, click **View Report**. The security scan report page is displayed.

Step 5 Click the **Base Images** tab and view reports.

You can view the name, version, and image layer path of a service image that is not created using a base image.

----End

Exporting Image Vulnerability or Baseline Report of SWR Enterprise Edition

NOTE

Vulnerability reports cannot be exported for multi-architecture images.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 3 Click **Enterprise Edition Images (SWR)** on the **Container Images** tab to view the image information.

Step 4 Click **Export Vulnerability** above the image list and select a report type to export the vulnerability or baseline report.

If you want to export the vulnerability report of a specified image, select the image type in the search box and click **Export Vulnerability**.

Step 5 View the export status in the upper part of the container management page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

3.5.5 Viewing Container Information

You can view container information on the **Containers** page to learn about the container status, cluster, and risks. This section describes how to view container information.

Constraints

- Only the HSS container edition supports this function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- Only the local images of the Docker engine can be reported to the HSS console.
- Security scans can be performed only on Linux images.

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Choose **Containers**. The container page is displayed.

Step 5 View the container information and security status.

In the container list, you can view the container name, status, risks, restart times, POD, and cluster.

- View container details.

  Click the name of the target container. On the container details page that is displayed, view the container image, process, port, and mount path information.
- View the container risk distribution.

  View the number of low-risk, medium-risk, high-risk, and critical risks in the container.

----End

3.5.6 Handling Risk Containers

Scenario

HSS can detect container security risks and classify them into the following types:

- Critical: malicious program
- High risk: ransomware attacks, malicious programs, reverse shells, escape attacks, and dangerous commands
- Medium risk: web shell, abnormal startup, process exception, and sensitive file access
- Low risk: brute-force attack

To prevent containers with medium or higher security risks from affecting other containers, you can isolate, suspend, or kill risky containers.

Constraints

- Only the HSS container edition supports this function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- Only Linux containers are supported.
- Only containers with medium or higher security risks can be handled.

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Choose **Containers**. The container page is displayed.

Step 5 Enter **Risk** in the search box and click 🔍 to filter containers with security risks.

Step 6 In the **Operation** column of the target risky container, select the operation to be performed.

Cluster containers can be killed. Single-node containers can be isolated, suspended, and killed.

NOTE

Only containers with medium or higher risks can be handled. You can view the security risk distribution.

- **Isolate containers**: After a container is isolated, you cannot access the container when the container is running, and the container cannot access the mount directory of the host or the system file of the container.

a. Click **Isolate**.

b. In the dialog box that is displayed, click **OK**.

- **Suspend containers**: Freeze the processes running in the container.

a. Click **Suspend**.

b. In the dialog box that is displayed, click **OK**.

- **Kill containers**: Terminate a running container process. If **autoremove** is configured for the container, the container cannot be resumed.

a. Click **Kill** to kill the container.

b. In the dialog box that is displayed, click **OK**.

----End

Related Operations

Restoring a container to the running state

Restores a container from the **Isolate**, **Waiting**, or **Terminated** state to the **Running** state.

NOTE

If **autoremove** is configured for a terminated container, the container cannot be resumed.

Step 1 In the row containing the target container, click **Restore** in the **Operation** column.

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

----End

3.5.7 Managing Cluster Agents

3.5.7.1 Installing an Agent

To install the agent for all containers in a CCE cluster or an on-premises Kubernetes cluster, you can use the cluster agent management function to install the agent in the cluster. After this function is enabled, you do not need to manually install the agent on new nodes or pods added to the cluster.

Installing an Agent in a CCE Cluster

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Cluster Agents** tab and click **CCE cluster**.

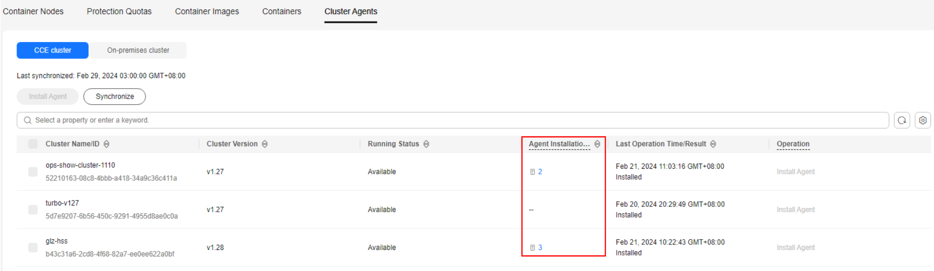
Step 5 In the **Operation** column of a cluster, click **Install Agent**.

You can also select multiple clusters and click **Install Agent** in the upper left corner of the list.

Step 6 In the dialog box that is displayed, click **OK**.

It takes about 10 minutes to install the agent. Wait for 10 minutes and move the cursor to the **Agent Installation Status** column to view the status. You can click the value of uninstalled or installed nodes to go to the details page of the corresponding cluster.

Figure 3-27 Checking the agent installation status



Last synchronized: Feb 29, 2024 03:00:00 GMT+08:00

Cluster Name/ID	Cluster Version	Running Status	Agent Installatio...	Last Operation Time/Result	Operation
ops-show-cluster-1110 52210163-08c8-4bbb-a418-34a9c36c411a	v1.27	Available	2	Feb 21, 2024 11:03:16 GMT+08:00 Installed	Install Agent
turbo-v127 5d7e9207-6b56-450c-9291-4955d8ae0c0a	v1.27	Available	--	Feb 20, 2024 20:29:49 GMT+08:00 Installed	Install Agent
glz-hss b43c31a6-2cd8-4f68-82a7-ee0ee622a0bf	v1.28	Available	3	Feb 21, 2024 10:22:43 GMT+08:00 Installed	Install Agent

----End

Installing an Agent in an On-Premises Cluster

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Cluster Agents** tab and click **On-premises cluster**.

Step 5 Click **Add On-Premises Cluster**.

Step 6 In the dialog box that is displayed, enter cluster information and click **Generate Command**.

In the dialog box that is displayed, click **Save**.

Step 7 Create a YAML file, for example, **abcd.yaml**, on the server where Kubernetes commands can be executed.

Step 8 Copy the generated command to **abcd.yaml**.

Step 9 Run the following command on the server to execute **abcd.yaml** and install the agent. This step takes about 10 minutes.

```
kubectl apply -f abcd.yaml
```

Step 10 Return to the HSS console.

Step 11 In the navigation pane, choose **Installation & Configuration**.

Step 12 Click the **Agents** tab. If the agent status of the cluster server is **Online**, the agent has been installed.

----End

Modifying On-premises Cluster Information

- To modify the on-premises cluster information or view commands, click **Edit** in its **Operation** column.
- To remove the information about an on-premises cluster, click **Remove** in its **Operation** column.

Follow-up Procedure

After the agent is installed, enable protection for the container. For details, see **Enabling Container Protection**.

3.5.7.2 Uninstalling an Agent from a Cluster

If you no longer need HSS to protect the containers in your cluster, uninstall the agent from the cluster. After the agent is uninstalled, HSS will stop checking and protecting containers, and the information about alarms and detected vulnerabilities will be deleted.

Uninstalling an Agent from a CCE Cluster

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Containers** > **Cloud Container Engine**. The CCE console is displayed.

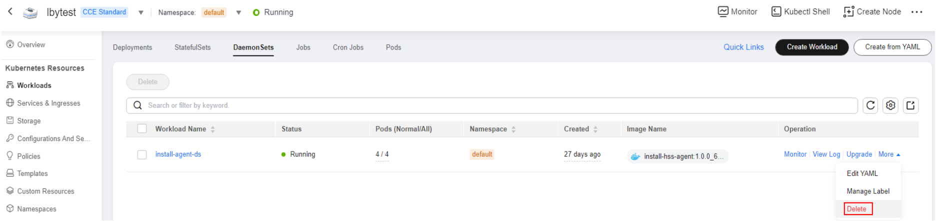
Step 3 Click the name of a cluster to enter its details page.

Step 4 In the navigation pane, choose **Workloads**.

Step 5 Click the **DaemonSet** tab and delete the workload **install-agent-ds**.

In the **Operation** column of the workload, choose **More** > **Delete**.

Figure 3-28 Deleting install-agent-ds



Workload Name	Status	Pods (Normal/All)	Namespace	Created	Image Name	Operation
install-agent-ds	Running	4 / 4	default	27 days ago	install-hss-agent:1.0.0_6...	Monitor | View Log | Upgrade | More

Step 6 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 7 In the navigation pane, choose **Installation & Configuration**.

Step 8 Click the **Agents** tab. Uninstall the agent from all container nodes in the CCE cluster.

For details, see **Uninstalling an Agent**.

----End

Uninstalling an Agent from an On-Premises Cluster

Step 1 Log in to the Kubernetes cluster.

Step 2 Run the following command to delete the workload **install-agent-ds**:

```
kubectl delete ds install-agent-ds -n default
```

Step 3 **Log in to the management console**.

Step 4 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 5 In the navigation pane, choose **Installation & Configuration**.

Step 6 Click the **Agents** tab. Uninstall the agent from all container nodes in the cluster.

For details, see **Uninstalling an Agent**.

----End

3.6 Protection Quota Management

3.6.1 Viewing Protection 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 Server 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 On the **Quotas** tab page, view HSS quotas. **Table 3-13** lists the related parameters.

Table 3-13 Parameter description

Parameter	Description
Quota ID	Unique ID of a quota.
Edition	● Basic ● Professional Edition ● Enterprise ● Premium ● Web Tamper Protection (WTP)
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.
Quota Status	● **Normal**: 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.
Billing Mode	● Yearly/Monthly ● Pay-per-use
Enterprise Project Name	Name of the enterprise project to which the target quota belongs
Tag	Resource category tag.

NOTE

- Binding quota to a server

  Alternatively, choose **Asset Management** > **Servers & Quota** from the left navigation pane, and click the **Quotas** tab. In the quota list displayed, click **Bind Server** in the **Operation** column to bind a quota to a server. HSS will automatically protect the server.

  A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- Unbind

  On the **Quotas** tab of the **Servers & Quota** page, click **Unbind** in the **Operation** column of a quota. HSS will no longer protect the server and the quota status will change to **Idle**.
- Export the quota list.

  Click ↗ in the upper right corner of the quota list to export the quota information on the current page.

----End

Viewing Container 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Containers & Quota**. On the displayed page, click the **Protection Quotas** tab.

Step 4 On the **Protection Quotas** tab page, view HSS protection quotas. **Table 3-14** lists the related parameters.

Table 3-14 Parameter description

Parameter	Description
Quota ID	Quota ID
Quota Version	Enterprise edition
Quota Status	● **Normal**: The quota is normal. ● **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.
Billing Mode	● Yearly/Monthly ● Pay-per-use
Tag	Resource category tag.

NOTE

- 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 Unsubscribe from HSS Quotas?**

----End

3.6.2 Binding a Protection Quota

You can bind a quota you purchased to a server to protect it.

Prerequisites

- The agent has been installed on the server, and the agent status is **Online**. For details about how to install the agent, see **Installing an Agent**.
- The quota is in **Normal** state and its **Usage Status** is **Idle**.
- A quota can be bound to a server to protect it, on condition that the agent on the server is online.

Manually Binding Quotas to a 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

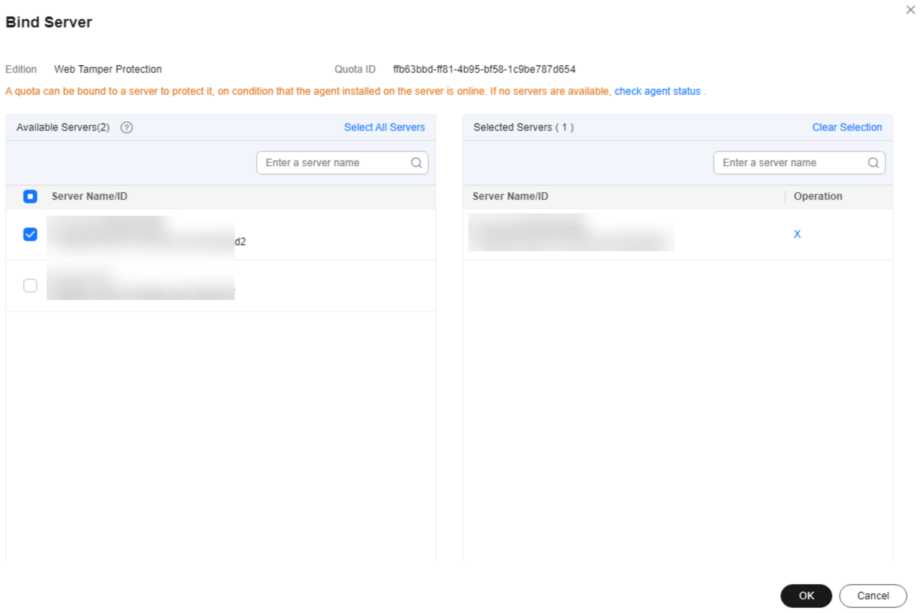
Step 4 On the **Quotas** tab page, locate the row that contains the target quota and click **Bind Server** in the **Operation** column.

NOTE

To bind a WTP quota to a server, choose **Prevention** > **Web Tamper Protection** from the navigation pane on the left. On the **Servers** tab page displayed, locate the row containing your desired server and click **Enable Protection** in the **Operation** column. HSS automatically enables WTP for the server.

Step 5 Select a server.

Figure 3-29 Selecting a server to be bound



Bind Server

Edition Web Tamper Protection Quota ID ffb63bbd-ff81-4b95-bf58-1c9be787d654

A quota can be bound to a server to protect it, on condition that the agent installed on the server is online. If no servers are available, check agent status .

Available Servers(2)

■	Server Name/ID
☑	[redacted]d2
□	[redacted]

Selected Servers (1)

Server Name/ID	Operation
[redacted]	X

Step 6 Click **OK**. HSS will automatically enable protection for the server.

----End

Manually Binding Quotas to a Container

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** > **HSS**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**. Click the **Protection Quotas** tab. The protection quota list page is displayed.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 On the **Quotas** tab page, locate the row that contains the target quota and click **Bind Server** in the **Operation** column.

Step 5 Select a server.

Step 6 Click **OK**. HSS will automatically enable protection.

----End

Automatically Binding Quotas

Automatic Binding Description

After automatic quota binding is enabled, HSS automatically binds available quotas to new servers or container nodes after the agent is installed for the first time. Only the yearly/monthly quotas that you have purchased can be automatically bound. No new order or fee is generated.

- Servers: Available yearly/monthly quotas are automatically bound in the following sequence: Premium Edition > Enterprise Edition > Professional Edition > Basic Edition.
- Container nodes: Available yearly/monthly quotas are automatically bound in the following sequence: Container Edition > Premium Edition > Enterprise Edition > Professional Edition > Basic Edition.
- If the version of the agent installed on the Linux server is 3.2.10 or later or the version of the agent installed on the Windows server is 4.0.22 or later, ransomware prevention is automatically enabled with the premium, WTP, or container edition. Deploy bait files on servers and automatically isolate suspicious encryption processes (there is a low probability that processes are incorrectly isolated). You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Enabling Ransomware Backup**.

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** > **HSS**.

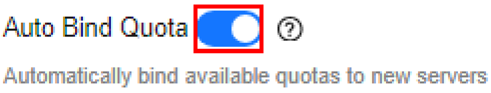
Step 3 In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**.

NOTE

You can also configure the automatic quota binding function on either the protection quota purchasing page or the container management page.

Step 4 Click to enable automatic quota binding.

Figure 3-30 Enabling automatic quota binding



Auto Bind Quota

Automatically bind available quotas to new servers

----End

3.6.3 Unbinding a Protection Quota

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.

Prerequisites

The quotas to be unbound are in use.

Unbinding a Quota from a 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 On the **Quotas** page, click **Unbind** in the **Operation** column of a quota.

To unbind quotas in batches, select the servers they bind to, and click **Batch Unbind** above the quota list.

NOTE

Exercise caution when performing this operation, because unprotected servers are exposed to security risks.

Step 5 In the confirmation dialog box, click **OK**.

----End

Unbinding a Container 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 On the **Quotas** page, click **Unbind** in the **Operation** column of a quota.

To unbind quotas in batches, select the servers they bind to, and click **Batch Unbind** above the quota list.

NOTE

Exercise caution when performing this operation, because unprotected servers are exposed to security risks.

Step 5 In the confirmation dialog box, click **OK**.

----End

3.6.4 Upgrading Protection Quotas

You can upgrade to a higher edition and enjoy stronger security features.

Precautions

- **Premium**, **Web Tamper Protection**, and **Container** are high-configuration editions and cannot be upgraded. You can purchase these quotas separately.
- **Basic**, **Professional**, and **Enterprise** can be upgraded to a higher quota edition.
  - **Basic**: can be upgraded to **Professional**, **Enterprise**, or **Premium**.
  - **Professional**: can be upgraded to **Enterprise** or **Premium**.
  - **Enterprise**: can be upgraded to **Premium**.

Prerequisites

- The **Usage Status** of a quota must be **Idle**.

- The **Quota Status** of a quota must be **Normal**.

Upgrading to the Professional/Enterprise/Premium Edition

To upgrade a quota that is being used to protect a server, unbind it from the server first.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

> NOTE
>
> If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

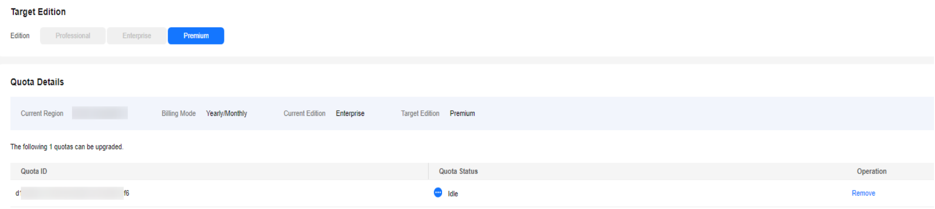
Step 4 In the quota list, filter the idle quotas of the basic or enterprise edition. Select a quota and click **Upgrade**.

> NOTE
>
> - Before upgrading a quota in use, **unbind it** from the server it protects.
> - Unbinding does not affect services.

Step 5 Configure upgrade information.

> NOTE
>
> The basic edition can be upgraded to the enterprise or premium edition. The enterprise edition is upgraded to the premium edition by default.

Figure 3-31 Confirming upgrade information



Target Edition

Edition: Professional | Enterprise | Premium

Quota Details

Current Region [redacted] Billing Mode Yearly/Monthly Current Edition Enterprise Target Edition Premium

The following 1 quotas can be upgraded.

Quota ID	Quota Status	Operation
d[redacted]f6	Idle	Remove

Step 6 Confirm the upgrade version and click **Next**.

> NOTE
>
> When you pay for the upgrade, you only need to make up the difference.

Step 7 Confirm the purchase information, select **I have read and agree to the Host Security Service Disclaimer**, and click **Pay Now**.

Step 8 Wait until the payment is complete. Return to the **quota list**. Locate the quota by its ID and check its edition.

Step 9 **Bind the quota** to a server and enable protection.

----End

Upgrading to the WTP Edition

The WTP edition cannot be directly upgraded from a lower edition and needs to be purchased separately. Before protecting a server with WTP, ensure the server is not bound to any 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** > **HSS**.

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

Step 4 On the **Buy HSS** page, select the WTP edition.

Table 3-15 Parameters for purchasing HSS

Parameter	Description	Example Value
Billing Mode	Select **Yearly/Monthly** or **Pay-per-use** billing mode based on your requirements. ● Yearly/Monthly: You can select the basic, professional, enterprise, premium, WTP, or container edition. You can purchase the edition for a fixed period of time. The fee is 30% lower than that of pay-per-use. If you use the edition for a long time, you are advised to purchase yearly/monthly packages. ● Pay-per-use: Only the enterprise edition can be purchased. You need to enable this edition in the server list. You pay for the duration you use the resources. Prices are calculated by hour, and no minimum fee is required. **NOTE** Procedure for enabling pay-per-use quota: 1. On the purchase page, select **Pay-per-use**. The **Enterprise** edition will be automatically selected. In the lower right corner, click **Enable Now**. You will be redirected to the server list. 2. In the server list, click **Enable** in the **Operation** column. Set the **Billing Mode** to **Pay-per-use** and **Edition** to **Enterprise**. 3. Confirm the information and click **OK**.	Yearly/Monthly
Region	● To minimize connection issues, purchase quota in the region of your servers.	CN-Hong Kong

Parameter	Description	Example Value
Edition	The **basic, professional, enterprise,premium,WTP,** and **container editions** are supported. For details about the differences between editions, see **Editions**. NOTICE ● If you enable the HSS basic edition for the first time, you can enjoy the free trial for 30 days and purchase it after the trial. ● If you purchased the basic, enterprise, or premium edition, enable it on the **Asset Management** > **Servers & Quota** page. ● If you purchased the WTP edition, enable it in the server list on the **Prevention** > **Web Tamper Protection** page. ● If you purchased the container edition, choose **Asset Management** > **Containers & Quota** and enable protection on the **Container Nodes** tab.	Enterprise
Enterprise Project	This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects. 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. Select an enterprise project from the drop-down list. NOTE ● Resources and incurred expenses are managed under the enterprise project you selected. ● 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. ● The **default** option is available in the **Enterprise Project** drop-down list only after you purchased HSS under your Huawei ID.	default
Required duration	● Select a duration based on your requirements. In **Pay-per-use** mode, you do not need to select a duration. ● 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.	1 year

Parameter	Description	Example Value
Server Quota	Enter the number of HSS quotas to be purchased. In **Pay-per-use** mode, you do not need to configure this option. **NOTICE** ● All your servers should be protected, so that if a virus (such as ransomware or a mining program) infects one of them, it will not be able to spread to others and damage your entire network. ● You cannot modify the quota of an edition after its purchase is complete. You can unsubscribe from it and purchase again.	20
Tag	Tags are used to identify cloud resources. When you have many cloud resources of the same type, you can use tags to classify cloud resources by dimension (for example, by usage, owner, or environment). To use this function, your account must have the **TMS administrator** permission. Without this permission, you cannot add tags to protection quotas, and the error message "permission error" will be displayed. You do not need to set this parameter in pay-per-use mode.	data
Quota Management	After automatic quota binding is enabled, HSS automatically binds available quotas to new servers or container nodes after the agent is installed for the first time. Only the yearly/monthly quotas that you have purchased can be automatically bound. No new order or fee is generated. ● Servers: Available yearly/monthly quotas are automatically bound in the following sequence: Premium Edition > Enterprise Edition > Professional Edition > Basic Edition. ● Container nodes: Available yearly/monthly quotas are automatically bound in the following sequence: Container Edition > Premium Edition > Enterprise Edition > Professional Edition > Basic Edition.	Selected

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 In the dialog box that is displayed, select a verification mode, click **Send Code**, enter the verification code you receive, and click **OK**.

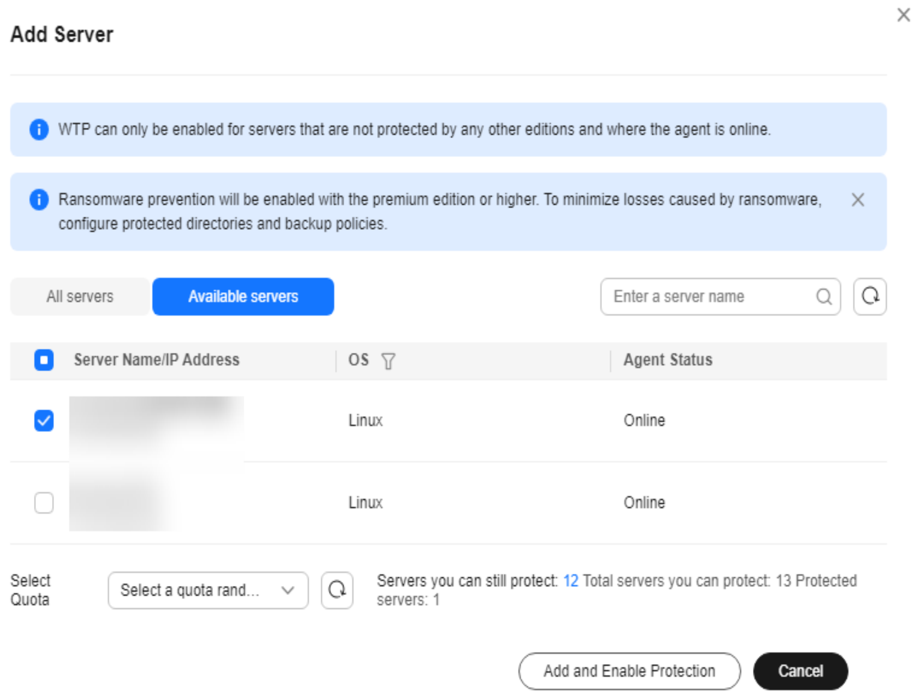
Step 8 In the navigation pane, choose **Prevention** > **Web Tamper Protection**. On the **Servers** tab, click **Add Server**.

NOTICE

- Ensure the server to be protected by WTP is not bound to other quotas. Choose **Asset Management** > **Servers & Quota** and click the **Servers** tab. If the protection status of the server is **Protected**, it indicates the server is bound to another quota. In this case, click **Disable** in the **Operation** column.
- Unbinding a server from a quota does not affect services.

Step 9 Click **Add Server**, select a server, and click **Add and Enable Protection**.

Figure 3-32 Selecting a server



Add Server

WTP can only be enabled for servers that are not protected by any other editions and where the agent is online.

Ransomware prevention will be enabled with the premium edition or higher. To minimize losses caused by ransomware, configure protected directories and backup policies.

☑ Server Name/IP Address	OS	Agent Status
☑ [redacted]	Linux	Online
□ [redacted]	Linux	Online

Select Quota: Select a quota rand...

Servers you can still protect: 12 Total servers you can protect: 13 Protected servers: 1

Step 10 Verify WTP configurations. Choose **Asset Management** > **Servers & Quota** and click the **Servers** tab. If **WTP** is displayed in the **Edition/Expiration Date** column, the WTP edition has been enabled.

NOTE

If you do not need the quota replaced by WTP, you can unsubscribe from it. Choose **Asset Management** > **Servers & Quota** and click the **Quotas** tab. In the **Operation** column of the quota, choose **More** > **Unsubscribe**.

----End

3.6.5 Exporting the Protection Quota List

This section describes how to export the server protection quota list to your local PC. Currently, the container protection quota list cannot be exported.

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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**.

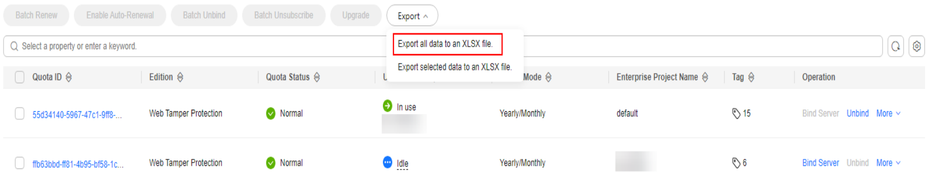
> **NOTE**
>
> If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the **Quotas** tab

Step 5 Above the protection quota list, click **Export** > **Export All Data to an XLSL file** to export the server protection quota list.

If you only need to export specified protection quota information, select the target quota and choose **Export** > **Export selected data to an XLSL file**.

Figure 3-33 Exporting all server protection quotas



Batch Renew
Enable Auto-Renewal
Batch Unbind
Batch Unsubscribe
Upgrade
Export ^
Export all data to an XLSX file.
Export selected data to an XLSX file.
Select a property or enter a keyword.

□	Quota ID	Edition	Quota Status	U	Mode	Enterprise Project Name	Tag	Operation
□	55d34140-5967-47c1-9ff8-...	Web Tamper Protection	✓ Normal	In use	Yearly/Monthly	default	15	Bind Server Unbind More
□	ffb63bbd-ff81-4b95-bf58-1c...	Web Tamper Protection	✓ Normal	Idle	Yearly/Monthly		6	Bind Server Unbind More

Step 6 View the export status in the upper part of the page. After the export is successful, obtain the exported information from the default file download address on the local host.

> **NOTICE**
>
> Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

4 Risk Prevention

4.1 Vulnerability Management

4.1.1 Vulnerability Management Overview

Vulnerability management can detect Linux, Windows, Web-CMS, application vulnerabilities, and emergency vulnerabilities and provide suggestions, helping you learn about server vulnerabilities in real time. Linux and Windows vulnerabilities can be fixed in one-click mode. This section describes how the vulnerabilities are detected and the vulnerabilities that can be scanned and fixed in each HSS edition.

NOTE

The vulnerability list displays vulnerabilities detected in the last seven days. After a vulnerability is detected for a server, if you change the server name and do not perform a vulnerability scan again, the vulnerability list still displays the original server name.

How Vulnerability Scan Works

Table 4-1 describes how different types of vulnerabilities are detected.

Table 4-1 How vulnerability scan works

Type	Mechanism
Linux vulnerability	Based on the vulnerability database, checks and handles vulnerabilities in the software (such as kernel, OpenSSL, vim, glibc) you obtained from official Linux sources and have not compiled, reports the results to the management console, and generates alarms.
Windows vulnerability	Synchronizes Microsoft official patches, 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.

Type	Mechanism
Web-CMS vulnerability	Checks web directories and files for Web-CMS vulnerabilities, reports the results to the management console, and generates vulnerability alarms.
Application vulnerability	Detects the vulnerabilities in the software and dependency packages running on the server, reports risky vulnerabilities to the console, and displays vulnerability alarms.
Emergency Vulnerabilities	Checks whether the software and any dependencies running on the server have vulnerabilities through version comparison and POC verification. Reports risky vulnerabilities to the console and provides vulnerability alarms for you.

Types of Vulnerabilities That Can Be Scanned and Fixed

For details about the types of vulnerabilities that can be scanned and fixed in different HSS editions, see **Types of vulnerabilities that can be scanned and fixed in each HSS edition**.

The meanings of the symbols in the table are as follows:

- √: supported
- ×: not supported

Table 4-2 Types of vulnerabilities that can be scanned and fixed in each HSS edition

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
Linux vulnerability	Automatic vulnerability scan (reporting based on the software asset collection period)	√	√	√	√	√	√

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	Scheduled vulnerability scan (By default, vulnerabilities are scanned once a week. You can change the scan period by configuring vulnerability policies.)	×	√	√	√	√	√
	Vulnerability whitelist	×	√	√	√	√	√
	Manual vulnerability scan	×	√	√	√	√	√
	One-click vulnerability fix	×	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√	√	√
Windows vulnerability	Automatic vulnerability scan (reporting based on the software asset collection period)	√	√	√	√	√	×

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	Scheduled vulnerability scan (By default, vulnerabilities are scanned once a week. You can change the scan period by configuring vulnerability policies.)	×	√	√	√	√	×
	Vulnerability whitelist	×	√	√	√	√	×
	Manual vulnerability scan	×	√	√	√	√	×
	One-click vulnerability fix	×	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√	√	×
Web-CMS vulnerability	Automatic vulnerability scan (reporting based on the software asset collection period)	×	√	√	√	√	√

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	Scheduled vulnerability scan (By default, vulnerabilities are scanned once a week. You can change the scan period by configuring vulnerability policies.)	×	√	√	√	√	√
	Vulnerability whitelist	×	√	√	√	√	√
	Manual vulnerability scan	×	√	√	√	√	√
	One-click vulnerability fix	×	×	×	×	×	×
Application vulnerability	Automatic vulnerability scan (reporting based on the middleware asset collection period)	×	×	√	√	√	√

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	Scheduled vulnerability scan (By default, vulnerabilities are scanned once a week. You can change the scan period by configuring vulnerability policies.)	×	×	√	√	√	√
	Vulnerability whitelist	×	×	√	√	√	√
	Manual vulnerability scan	×	×	√	√	√	√
	One-click vulnerability fix	×	×	×	×	×	×
Emergency vulnerability	Automatic vulnerability scan	×	×	×	×	×	×
	Scheduled vulnerability scan (This function is disabled by default and can be enabled through vulnerability policy configuration.)	×	√	√	√	√	√
	Vulnerability whitelist	×	× ×	×	×	×	×

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	Manual vulnerability scan	×	√	√	√	√	√
	One-click vulnerability fix	×	×	×	×	×	×

NOTE

HSS can scan for Web-CMS , emergency vulnerabilities, and application vulnerabilities but cannot fix them. You can log in to your server to manually fix the vulnerability by referring to the suggestions displayed on the vulnerability details page.

4.1.2 Vulnerability Scan

HSS can scan for Linux, Windows, Web-CMS, application vulnerabilities, and emergency vulnerabilities. Automatic, scheduled (vulnerability policy configuration), and manual scans are supported.

- Automatic scan

  When collecting asset fingerprints, HSS automatically scans vulnerabilities. For Linux, Windows, and Web-CMS vulnerabilities, HSS scans them based on the software collection period. For application vulnerabilities, HSS scans them based on the middleware collection period. For details about the asset fingerprint collection period, see **Collecting Server Asset Fingerprints**.

  If vulnerabilities have been manually scanned or a scheduled vulnerability scanning task has been triggered within the asset fingerprint collection period, HSS will automatically scan vulnerabilities when collecting asset fingerprints next time. This collection mode is affected by the other two scanning modes, and the scanning period is not fixed. You are advised to use the other two scan methods.

- Scheduled scan

  By default, HSS performs a full server vulnerability scan once a week. To ensure service security, you are advised to set a proper scan period and scan server scope to periodically scan server vulnerabilities.

- Manual scan

  If you want to view the vulnerability fixing status or real-time vulnerabilities of a server, you are advised to manually scan for vulnerabilities.

This section describes how to manually scan for vulnerabilities and configure a scheduled scan policy.

Constraints

- If the agent version of the Windows OS is 4.0.18 or later, application vulnerability scan is supported. If the agent version of the Linux OS is 3.2.9 or later, emergency vulnerability scan is supported. For details about how to upgrade the agent, see **Upgrading the Agent**.
- The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**. Otherwise, vulnerability scan cannot be performed.
- For details about the types of vulnerabilities that can be scanned by different HSS editions, see **Types of Vulnerabilities That Can Be Scanned and Fixed**.
- For details about the OSs supportedby Linux and Windows vulnerability scan, see **Table 4-3**. Emergency vulnerability scan supports Ubuntu, CentOS, EulerOS, Debian, and AlmaLinux.

Table 4-3 OSs supporting vulnerability scan

OS Type	Supported OS
Windows	• Windows Server 2019 Datacenter 64-bit English (40 GB) • Windows Server 2019 Datacenter 64-bit Chinese (40 GB) • Windows Server 2016 Standard 64-bit English (40 GB) • Windows Server 2016 Standard 64-bit Chinese (40 GB) • Windows Server 2016 Datacenter 64-bit English (40 GB) • Windows Server 2016 Datacenter 64-bit Chinese (40 GB) • Windows Server 2012 R2 Standard 64-bit English (40 GB) • Windows Server 2012 R2 Standard 64-bit Chinese (40 GB) • Windows Server 2012 R2 Datacenter 64-bit English (40 GB) • Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)
Linux	• EulerOS 2.2, 2.3, 2.5, 2.8, and 2.9 (64-bit) • CentOS 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 (64-bit) • Ubuntu 16.04, 18.04, 20.04, 22.04 (64-bit) • Debian 9, 10, and 11 (64-bit) • Kylin V10 (64-bit) • HCE 1.1 and 2.0 (64-bit) • SUSE Linux 12 SP5, 15 SP1, 15 SP2 and 15.5 (64-bit) • UnionTech OS V20 server E and V20 server D (64-bit)

Manual Vulnerability Scan

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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 Click **Scan** in the upper right corner of the **Vulnerabilities** page.

To scan emergency vulnerabilities, locate the row of an emergency vulnerability, and click **Scan** in the **Operation**.

Step 5 In the **Scan for Vulnerability** dialog box displayed, select the vulnerability type and scope to be scanned. For more information, see Table 4-4.

Table 4-4 Parameters for manual scan vulnerabilities

Parameter	Description
Type	Select one or more types of vulnerabilities to be scanned. Possible values are as follows: ● **Linux** ● **Windows** ● **Web-CMS** ● **Application** ● **Emergency**
Scan	Select the servers to be scanned. Possible values are as follows: ● **All servers** ● **Selected servers** You can select a server group or search for the target server by server name, ID, EIP, or private IP address. **NOTE** The following servers cannot be selected for vulnerability scan: ● Servers are protected by basic edition HSS. ● Servers that are not in the **Running** state ● Servers whose agent status is **Offline**

Step 6 Click **OK**.

Step 7 Click **Manage Task** in the upper right corner of the **Vulnerabilities** page. On the **Manage Task** slide-out panel displayed, click the **Scan Tasks** tab to view the status and scan result of the vulnerability scan task.

Click the number next to the red figure in the **Scan Result** column to view information about the servers that fail to be scanned.

NOTE

You can also choose **Asset Management** > **Servers & Quota** and scan a single server for vulnerabilities on the **Servers** tab. The procedure is as follows:

1. Click a server name.
2. Choose **Vulnerabilities**.
3. Choose the vulnerability type to be scanned and click **Scan**.

----End

Scheduled Vulnerability Scanning (Vulnerability Policy Configuration)

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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 In the upper right corner of the **Vulnerabilities** page, click **Configure Policy** to set the vulnerability scan period and scope.

- **Vulnerability Type**
- **Scan Period**
  - **Scan period**: The default value is **00:00:00 - 07:00:00** and cannot be changed.
  - **Scan Period**: Select **Every day**, **Every three days**, or **Every week**.
- **Scan**
  - Enable or disable server scan: ● indicates that server scan is enabled.
  - Select the servers to scan: Click **Select Server to Scan**. On the server management page displayed, select the servers to be scanned.

    NOTE

    The following servers cannot be selected for vulnerability scan:

    - Servers are protected by basic edition HSS.
    - Servers that are not in the **Running** state
    - Servers whose agent status is **Offline**

Step 5 Click **Manage Task** in the upper right corner of the **Vulnerabilities** page. On the **Manage Task** slide-out panel displayed, click the **Scan Tasks** tab to view the status and scan result of the vulnerability scan task.

Click the number next to the red figure in the **Scan Result** column to view information about the servers that fail to be scanned.

----End

4.1.3 Viewing Vulnerability Details

You can view vulnerabilities of your assets on the **Vulnerabilities** page. The **Vulnerabilities** page contains two tabs: **Vulnerabilities view** and **Server view**, helping you analyze vulnerabilities from the vulnerability and server perspectives.

Constraints

- Servers that are not protected by HSS do not support this function.
- The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**. Otherwise, vulnerability scan cannot be performed.

Viewing Vulnerability Details (Vulnerability View)

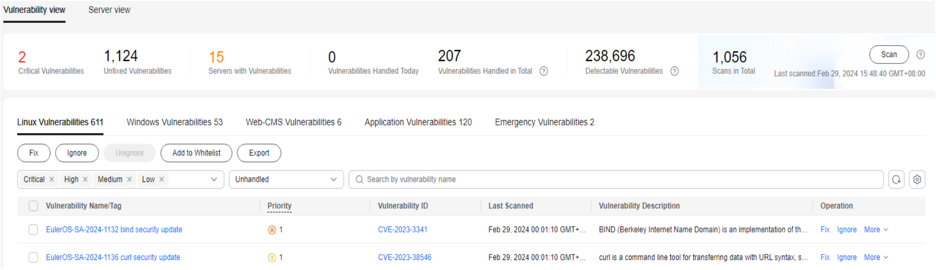
Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 View vulnerability information on the **Vulnerabilities** page.

Figure 4-1 Viewing vulnerability details


Vulnerability view
Server view
2
Critical Vulnerabilities
1,124
Unfixed Vulnerabilities
15
Servers with Vulnerabilities
0
Vulnerabilities Handled Today
207
Vulnerabilities Handled in Total
238,696
Detectable Vulnerabilities
1,056
Scans in Total
Scan
Last scanned:Feb 29, 2024 15:48:40 GMT+08:00
Linux Vulnerabilities 611
Windows Vulnerabilities 53
Web-CMS Vulnerabilities 6
Application Vulnerabilities 120
Emergency Vulnerabilities 2
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical
High
Medium
Low
Unhandled
Search by vulnerability name

Vulnerability Name/Tag	Priority	Vulnerability ID	Last Scanned	Vulnerability Description	Operation
EulerOS-SA-2024-1132 bind security update	1	CVE-2023-3341	Feb 29, 2024 00:01:10 GMT+...	BIND (Berkeley Internet Name Domain) is an implementation of th...	Fix Ignore More
EulerOS-SA-2024-1136 curl security update	1	CVE-2023-38546	Feb 29, 2024 00:01:10 GMT+...	curl is a command line tool for transferring data with URL syntax, s...	Fix Ignore More

- Viewing vulnerability scan results

  In the vulnerability statistics area in the upper part of the **Vulnerabilities** page, view vulnerability scan results. Table 4-5 describes related parameters.

Table 4-5 Vulnerability scan parameters

Parameter	Description
Critical Vulnerabilities	Click the number in **Critical vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities to be urgently fixed.
Unfixed Vulnerabilities	Click the number in **Unfixed Vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities that are not fixed.
Servers with Vulnerabilities	Click the number in **Servers with Vulnerabilities**. You can view the servers with vulnerabilities in the lower part of the **Vulnerabilities** page.
Vulnerabilities Handled Today	Click the number in **Vulnerabilities Handled Today**. On the slide-out panel displayed, you can view all types of vulnerabilities that have been handled today.
Vulnerabilities Handled in Total	Click the number in **Vulnerabilities Handled in Total**. On the slide-out panel displayed, you can view all types of vulnerabilities that have been handled. The number is just the quantity of vulnerabilities handled within one year.
Detectable Vulnerabilities	Displays the number of vulnerabilities that can be detected by HSS.

Parameter	Description
Scans in Total	Displays the number of vulnerability scans. Click **Scan** to manually scan for vulnerabilities on servers.

- Viewing vulnerability details

  Click the name of a target vulnerability. On the vulnerability details slide-out panel displayed, you can view the repair suggestions, CVE details, affected servers, and historical handling records of the vulnerability.

  For an affected server, you can view the server status and OS version.

- Viewing handled vulnerabilities or vulnerabilities to be handled

  Above the vulnerability list, select **Unhandled** or **Handled** from the vulnerability handling status drop-down list to filter vulnerabilities to be handled or that have been handled.

- Exporting the vulnerability list

  Click **Export** above the vulnerability list to export vulnerability data with just one-click. Then, you can view vulnerability information on your local PC.

  NOTE

  A maximum of 30,000 vulnerabilities can be exported at a time.

----End

Viewing Vulnerability Details (Server View)

NOTE

The basic edition does not support this operation.

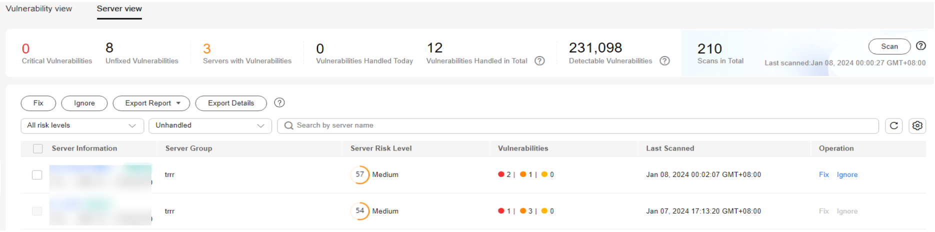
Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 In the upper left corner of the **Vulnerabilities** page, click **Server view** to view vulnerability information.

Figure 4-2 Viewing vulnerability details



0 Critical Vulnerabilities | 8 Unfixed Vulnerabilities | 3 Servers with Vulnerabilities | 0 Vulnerabilities Handled Today | 12 Vulnerabilities Handled in Total | 231,098 Detectable Vulnerabilities | 210 Scans in Total

Last scanned:Jan 08, 2024 00:00:27 GMT+08:00

Server Information	Server Group	Server Risk Level	Vulnerabilities	Last Scanned	Operation
[redacted]	trrr	57 Medium	● 2 | ● 1 | ● 0	Jan 08, 2024 00:02:07 GMT+08:00	Fix Ignore
[redacted]	trrr	54 Medium	● 1 | ● 3 | ● 0	Jan 07, 2024 17:13:20 GMT+08:00	Fix Ignore

- Viewing vulnerability scan results

In the vulnerability statistics area in the upper part of the **Vulnerabilities** page, view vulnerability scan results. **Table 4-6** describes related parameters.

Table 4-6 Vulnerability scan parameters

Parameter	Description
Critical vulnerabilities	Click the number in **Critical vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities to be urgently fixed.
Unfixed Vulnerabilities	Click the number in **Unfixed Vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities that are not fixed.
Servers with Vulnerabilities	Displays the number of servers with vulnerabilities.
Vulnerabilities Handled Today	Click the number in **Vulnerabilities Handled Today**. On the slide-out panel displayed, you can view all types of vulnerabilities that have been handled today.
Vulnerabilities Handled in Total	Click the number in **Vulnerabilities Handled in Total**. On the slide-out panel displayed, you can view all types of vulnerabilities that have been handled.
Detectable Vulnerabilities	Displays the number of vulnerabilities that can be detected by HSS.
Scans in Total	Displays the number of vulnerability scans. Click **Scan** to manually scan for vulnerabilities on servers.

- Viewing server details and vulnerabilities on servers

  a. Click the name of a target server. On the server details slide-out panel displayed, you can view details about the server and vulnerabilities on the server.

  b. Click the name of a target vulnerability. On the vulnerability details slide-out panel displayed, you can view the CVE details, affected servers, and historical handling records of the vulnerability.

- Viewing handled vulnerabilities or vulnerabilities to be handled

  Above the vulnerability list, select **Unhandled** or **Handled** from the vulnerability handling status drop-down list to filter vulnerabilities to be handled or that have been handled.

- Exporting the list of servers with vulnerabilities

  Click **Export** above the vulnerability list to export vulnerability data with just one-click. Then, you can view vulnerability information on your local PC.

  NOTE

  A maximum of 30,000 vulnerabilities can be exported at a time.

----End

4.1.4 Exporting the vulnerability list

You can refer to this section to export the vulnerability list.

Prerequisite

- HSS professional or later edition has been enabled for the server.
- The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**.

Exporting the Vulnerability List (Vulnerability View)

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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 In the upper left corner of the **Vulnerabilities** page, click the **Vulnerability view** tab.

Step 5 Click **Export** above the vulnerability list to export the vulnerability list.

Step 6 View the export status in the upper part of the **Vulnerabilities** page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

Exporting the Vulnerability List (Server View)

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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 In the upper left corner of the **Vulnerabilities** page, click the **Server view** tab.

Step 5 Export the vulnerability list.

- Export vulnerability details: In the upper part of the vulnerability list, click **Export Details** to export the vulnerability list.
- Export a vulnerability report: In the upper part of the vulnerability list, click **Export Report** and select a report format.

NOTE

- When exporting a vulnerability report in HTML format, the vulnerability information about up to 100 servers can be exported.
- When exporting a vulnerability report in PDF format, the vulnerability information about up to 140 servers and vulnerabilities can be exported.
- You can also select target servers and export their vulnerability information.

Step 6 View the export status in the upper part of the **Vulnerabilities** page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

4.1.5 Handling Vulnerabilities

If HSS detects a vulnerability on a server, you need to handle the vulnerability in a timely manner based on its severity and your business conditions to prevent the vulnerability from being exploited by intruders.

Vulnerabilities can be handled in the following ways:

- **Fixing vulnerabilities**

  If a vulnerability may harm your services, fix it as soon as possible. For Linux and Windows vulnerabilities, you can let HSS fix them in one-click. Web-CMS vulnerabilities, emergency vulnerabilities, and application vulnerabilities cannot be automatically fixed. Handle them by referring to the suggestions provided on the vulnerability details page.
- **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. If you can confirm that a vulnerability is harmless, you can ignore it. If the vulnerability is detected again in the next vulnerability scan, HSS will still report it.
- **Adding vulnerabilities to the whitelist**

  If you can confirm that a vulnerability does not affect your services and does not need to be fixed, you can add it to the whitelist. After a vulnerability is added to the whitelist, its status will change to **Ignored** in the vulnerability list, and it will not be reported in later scans.

Constraints

- For details about vulnerability handling operations supported by each HSS version, see **Types of Vulnerabilities That Can Be Scanned and Fixed**.
- CentOS 6 and CentOS 8 are officially End of Life (EOL) and no longer maintained. HSS scans them for vulnerabilities based on Red Hat patch notices but cannot fix them. You are advised to change to other OSs.

- Ubuntu 18.04 and earlier versions do not support free patch updates. You need to purchase and configure Ubuntu Pro to install upgrade packages, or vulnerability fix will fail.
- The kernel vulnerabilities on CCE, MRS, and BMS servers cannot be fixed. Fixing them may make some functions unavailable.
- Kernel vulnerabilities of CCE hosts cannot be automatically fixed. HSS automatically filters out such vulnerabilities when fixing vulnerability in batches.
- To handle vulnerabilities on a server, ensure the server is in the **Running** state, its agent status is **Online**, and its protection status is **Protected**.

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 prevent unexpected consequences, you are advised to use CBR to back up ECSs. For details, see **Purchasing a Server Backup Vault**. 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 the server cannot access the Internet or the services provided by the external image source are unstable, you can use the image source provided by Huawei Cloud to fix vulnerabilities. To ensure that the vulnerability is successfully fixed, ensure that the image source . For details, see **Configuring the Image Source**.

Vulnerability Fix Priority

The vulnerability fix priority is weighted based on the CVSS score, release time, and the importance of the assets affected by the vulnerability. It reflects the urgency of the fix.

classifies vulnerability fix priorities into four levels: critical, high, medium, and low. You can refer to the priorities to fix the vulnerabilities that have significant impact on your server first.

- **Critical**: This vulnerability must be fixed immediately. Attackers may exploit this vulnerability to cause great damage to the server.
- **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.
- **Low**: This vulnerability has a small threat to server security. You can choose to fix or ignore it.

Vulnerability Display

Detected vulnerabilities will be displayed in the vulnerability list for seven days, regardless of whether you have handled them.

Handling Vulnerabilities

You can handle the vulnerability in following ways:

Automatically Fixing Vulnerabilities (Vulnerability View)

You can only fix Linux and Windows vulnerabilities with one-click on the console.

NOTE

A maximum of 1,000 server vulnerabilities can be fixed at a time. If there are more than 1,000 vulnerabilities, fix them in batches.

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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 Fix Linux and Windows vulnerabilities.

- Fixing a single vulnerability

  Locate the row containing a target vulnerability and click **Fix** in the **Operation** column.

- Fixing multiple vulnerabilities

  Select all target vulnerabilities and click **Fix** in the upper left corner of the vulnerability list to fix vulnerabilities in batches.

- Fix all vulnerabilities.

  Click **Fix** in the upper left corner of the vulnerability list to fix all vulnerabilities.

- Fix one or more servers affected by a vulnerability.

  a. Click a vulnerability name.

  b. On the vulnerability details slide-out panel displayed, click the **Affected** tab, locate the row containing the target server, and click **Fix** in the **Operation** column.

     You can also select all target servers and click **Fix** above the server list to fix vulnerabilities for the servers in batches.

Step 5 In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets.

For Linux vulnerabilities, you can click **View details** in the **Fix** dialog box to view the name of the component to be fixed.

Step 6 (Optional) Back up servers.

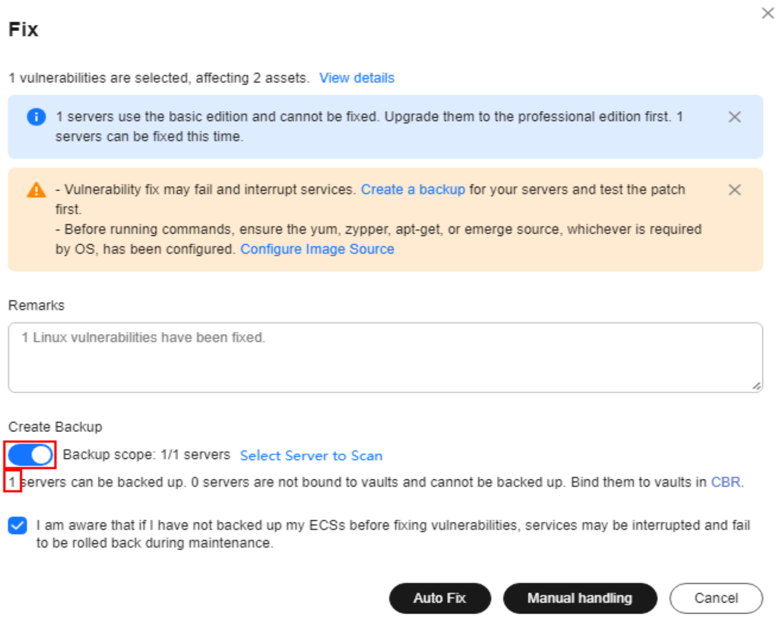
Before fixing vulnerabilities, use HSS to back up servers, so that you can restore their data if it is affected by the fix. If you do not need to back up data, skip this step.

1. In the **Fix** dialog box, click ○ to enable backup.

NOTE

- After backup is enabled, the number of servers that can be backed up will be displayed below the toggle switch. Only the servers associated with backup vaults can be backed up. For more information, see **Associating a Resource with the Vault**.
- If backup is enabled in a vulnerability fix task, vulnerabilities can be fixed only on the servers that can be backed up in this task. For servers that fail to be backed up, start another vulnerability fix task for them.

Figure 4-3 Creating a backup



Fix

1 vulnerabilities are selected, affecting 2 assets. View details

1 servers use the basic edition and cannot be fixed. Upgrade them to the professional edition first. 1 servers can be fixed this time.

- Vulnerability fix may fail and interrupt services. Create a backup for your servers and test the patch first.
- Before running commands, ensure the yum, zypper, apt-get, or emerge source, whichever is required by OS, has been configured. Configure Image Source

Remarks

1 Linux vulnerabilities have been fixed.

Create Backup

Backup scope: 1/1 servers Select Server to Scan

1 servers can be backed up. 0 servers are not bound to vaults and cannot be backed up. Bind them to vaults in CBR.

☑ 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.

2. Choose **Select Server to Scan**. The backup creation dialog box is displayed.
3. In the **Create Backup** dialog box, select a backup vault, set a backup file name, and click **OK**.

Step 7 In the **Fix** dialog box 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.** and click **Auto Fix**.

Step 8 Click a vulnerability name.

Step 9 Click the **Handling History** tab to view the fix status of the target vulnerability in the **Status** column. **Table 4-7** describes vulnerability fix statuses.

Table 4-7 Vulnerability fix statuses

Status	Description
Unhandled	The vulnerability is not fixed.
Ignored	The vulnerability does not affect your services. You have ignored the vulnerability.

Status	Description
Verifying	HSS is verifying whether a fixed vulnerability is successfully fixed.
Fixing	HSS is fixing the vulnerability.
Fixed	The vulnerability has been successfully fixed.
Restart required	The vulnerability has been successfully fixed. You need to restart the server as soon as possible.
Failed	The vulnerability fails to be fixed. The possible cause is that the vulnerability does not exist or has been changed.
Restart the server and try again	This status is displayed only for vulnerabilities that exist on Windows servers. The vulnerability has not been fixed on the Windows server for a long time. As a result, the latest patch cannot be installed. You need to install an earlier patch, restart the server, and then install the latest patch.

----End

Automatically Fixing Vulnerabilities (Server View)

You can only fix Linux and Windows vulnerabilities with one-click on the console.

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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 Fix Linux and Windows vulnerabilities.

- Fixing all vulnerabilities on a server

  a. Locate the row containing a target server and click **Fix** in the **Operation** column.

     You can also select multiple servers and click **Fix** in the upper part of the vulnerability list. To fix all server vulnerabilities, you just need to click **Fix** with no need of selecting servers.

  b. In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets.

     For Linux vulnerabilities, you can view fix commands in the dialog box to view the name of the component to be fixed.

  c. (Optional) Back up servers.

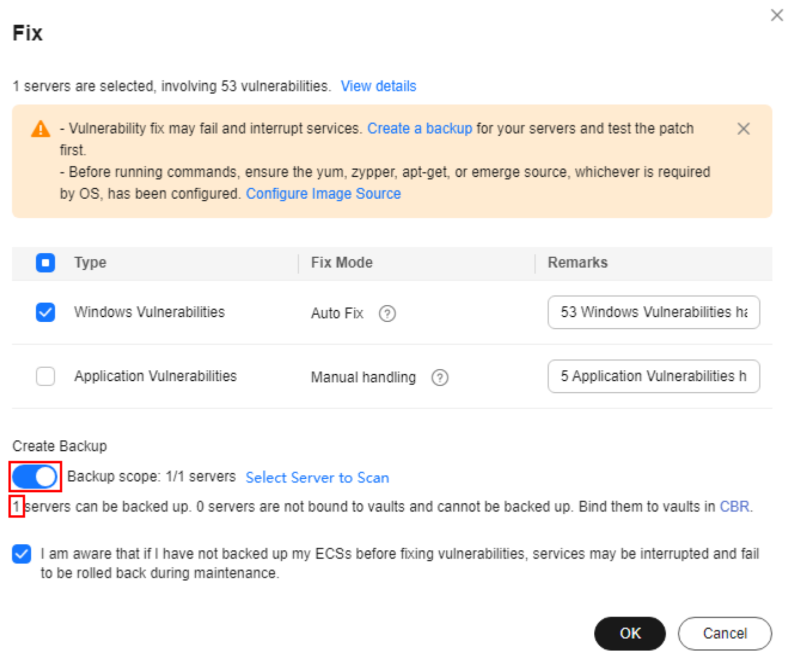
     Before fixing vulnerabilities, use HSS to back up servers, so that you can restore their data if it is affected by the fix. If you do not need to back up data, skip this step.

i. In the **Fix** dialog box, click to enable backup.

NOTE

- After backup is enabled, the number of servers that can be backed up will be displayed below the toggle switch. Only the servers associated with backup vaults can be backed up. For more information, see **Associating a Resource with the Vault**.
- If backup is enabled in a vulnerability fix task, vulnerabilities can be fixed only on the servers that can be backed up in this task. For servers that fail to be backed up, start another vulnerability fix task for them.

Figure 4-4 Creating a configuration backup



Fix

1 servers are selected, involving 53 vulnerabilities. View details

- Vulnerability fix may fail and interrupt services. Create a backup for your servers and test the patch first.
- Before running commands, ensure the yum, zypper, apt-get, or emerge source, whichever is required by OS, has been configured. Configure Image Source

■ Type	Fix Mode	Remarks
☑ Windows Vulnerabilities	Auto Fix ⓘ	53 Windows Vulnerabilities ha
□ Application Vulnerabilities	Manual handling ⓘ	5 Application Vulnerabilities h

Create Backup

Backup scope: 1/1 servers Select Server to Scan

1 servers can be backed up. 0 servers are not bound to vaults and cannot be backed up. Bind them to vaults in CBR.

☑ 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.

ii. Choose **Select Server to Scan**. The backup creation dialog box is displayed.

iii. In the **Create Backup** dialog box, select a backup vault, set a backup file name, and click **OK**.

d. In the **Fix** dialog box displayed, select the type of the vulnerability to be fixed, 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.**, and click **OK**.

Only Linux and Windows vulnerabilities can be automatically fixed with one-click. Web-CMS and application vulnerabilities need to be manually fixed by logging in to the server.

e. Click the server name. On the server details slide-out panel displayed, view the vulnerability fix status. **Table 4-8** describes vulnerability fix statuses.

- Fixing one or more vulnerabilities on a server

a. Click the name of a target server. The server details slide-out panel is displayed.

b. Locate the row containing a target vulnerability and click **Fix** in the **Operation** column.

   Alternatively, you can select all target vulnerabilities and click **Fix** above the vulnerability list to fix vulnerabilities in batches. To fix vulnerabilities of all servers, click **Fix** with no need of selecting any servers.

c. In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets.

   For Linux vulnerabilities, you can view fix commands in the dialog box to view the name of the component to be fixed.

d. (Optional) Back up servers.

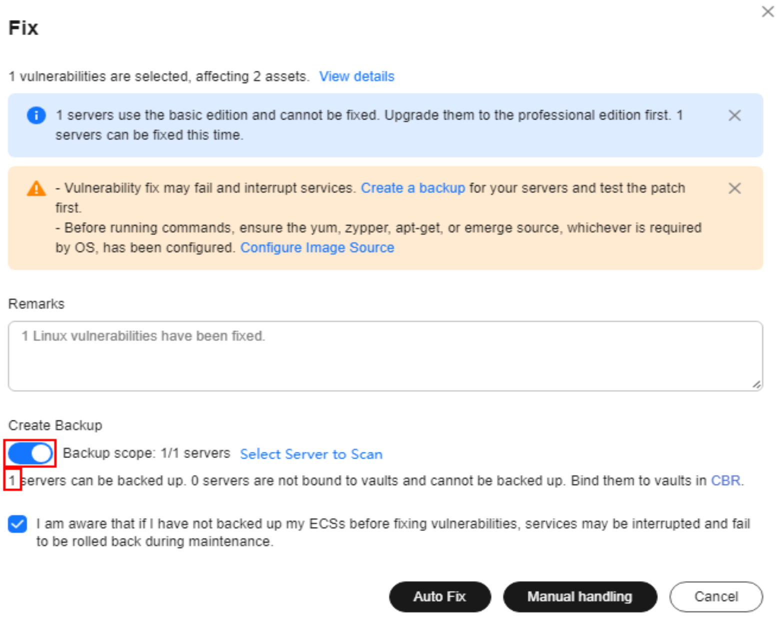
   Before fixing vulnerabilities, you can use HSS to back up servers, so that you can restore their data if it is affected by the fix. If you do not need to back up data, skip this step.

   i. In the **Fix** dialog box, click ○ to enable backup.

   NOTE

   - After backup is enabled, the number of servers that can be backed up will be displayed below the toggle switch. Only the servers associated with backup vaults can be backed up. For more information, see **Associating a Resource with the Vault**.
   - If backup is enabled in a vulnerability fix task, vulnerabilities can be fixed only on the servers that can be backed up in this task. For servers that fail to be backed up, start another vulnerability fix task for them.

Figure 4-5 Creating a backup



Fix

1 vulnerabilities are selected, affecting 2 assets. View details

1 servers use the basic edition and cannot be fixed. Upgrade them to the professional edition first. 1 servers can be fixed this time.

- Vulnerability fix may fail and interrupt services. Create a backup for your servers and test the patch first.
- Before running commands, ensure the yum, zypper, apt-get, or emerge source, whichever is required by OS, has been configured. Configure Image Source

Remarks

1 Linux vulnerabilities have been fixed.

Create Backup

Backup scope: 1/1 servers Select Server to Scan

1 servers can be backed up. 0 servers are not bound to vaults and cannot be backed up. Bind them to vaults in CBR.

☑ 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.

   ii. Choose **Select Server to Scan**. The backup creation dialog box is displayed.

   iii. In the **Create Backup** dialog box, select a backup vault, set a backup file name, and click **OK**.

e. In the **Fix** dialog box 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.**, and click **Auto Fix**.

f. In the **Status** column of the target vulnerability, view the fix status of the vulnerability. **Table 4-8** describes vulnerability fix statuses.

Table 4-8 Vulnerability fix statuses

Status	Description
Unhandled	The vulnerability is not fixed.
Ignored	The vulnerability does not affect your services. You have ignored the vulnerability.
Verifying	HSS is verifying whether a fixed vulnerability is successfully fixed.
Fixing	HSS is fixing the vulnerability.
Fixed	The vulnerability has been successfully fixed.
Restart required	The vulnerability has been successfully fixed. You need to restart the server as soon as possible.
Failed	The vulnerability fails to be fixed. The possible cause is that the vulnerability does not exist or has been changed.
Restart the server and try again	This status is displayed only for vulnerabilities that exist on Windows servers. The vulnerability has not been fixed on the Windows server for a long time. As a result, the latest patch cannot be installed. You need to install an earlier patch, restart the server, and then install the latest patch.

----End

Manually Fixing Vulnerabilities

HSS does not automatically fix Web-CMS vulnerabilities, application vulnerabilities, and emergency vulnerabilities with one-click. You can log in to the server to manually fix them by referring to the fix suggestions on the vulnerability details slide-out panel.

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.
- 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.

Viewing vulnerability fix suggestions

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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 Click the name of a target vulnerability to access the vulnerability details slide-out panel and view the fix suggestions.

----End

Fixing vulnerabilities by referring to vulnerability fix suggestions

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

- Method 1: Create a new VM to fix the vulnerability.
  a. Create an image for the ECS to be fixed. For details, see **Creating a Full-ECS Image Using an ECS**.
  b. Use the image to create an ECS. For details, see **Creating ECSs Using an Image**.
  c. Fix the vulnerability on the new ECS and verify the result.
  d. Switch services over to the new ECS and verify they are stably running.
  e. 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.
  a. Create a backup for the ECS whose vulnerabilities need to be fixed. For details, see **Creating a CSBS Backup**.
  b. Fix vulnerabilities on the current server.
  c. 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**.

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.
- After the vulnerability is manually fixed, you are advised to **Verify the Vulnerability Fix**.

Ignoring a Vulnerability

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.

After the vulnerability is ignored, no alarm will be generated for the vulnerability.

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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 Locate the row containing a target vulnerability and click **Ignore** in the **Operation** column.

Step 5 In the dialog box displayed, click **OK**.

----End

Whitelisting Vulnerabilities

If you evaluate that some vulnerabilities do not affect your services and do not want to view the vulnerabilities in the vulnerability list, you can whitelist the vulnerabilities. After they are whitelisted, the vulnerabilities will be ignored in the vulnerability list and no alarms will be reported. The vulnerabilities will not be scanned and the vulnerability information will not be displayed when the next vulnerability scan task is executed.

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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

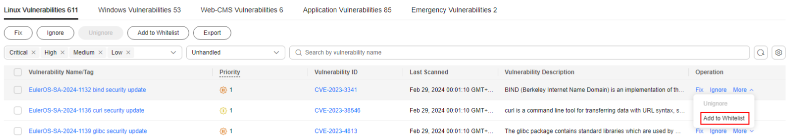
- Whitelisting all servers that are affected by a vulnerability

  HSS will ignore the vulnerability when scanning for vulnerabilities on all servers.

  a. In the **Operation** column of the row containing the target vulnerability, click **More** and select **Add to Whitelist**.

     You can also select multiple vulnerabilities and click **Add to Whitelist** above the vulnerability list.

     Figure 4-6 Whitelisting all servers that are affected by a vulnerability

     
     Linux Vulnerabilities 611
Windows Vulnerabilities 53
Web-CMS Vulnerabilities 6
Application Vulnerabilities 85
Emergency Vulnerabilities 2
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical ×
High ×
Medium ×
Low ×
Unhandled
Search by vulnerability name
Unignore
Add to Whitelist

Vulnerability Name/Tag	Priority	Vulnerability ID	Last Scanned	Vulnerability Description	Operation
EulerOS-SA-2024-1132 bind security update	1	CVE-2023-3341	Feb 29, 2024 00:01:10 GMT+...	BIND (Berkeley Internet Name Domain) is an implementation of th...	Fix Ignore More
EulerOS-SA-2024-1136 curl security update	1	CVE-2023-38546	Feb 29, 2024 00:01:10 GMT+...	curl is a command line tool for transferring data with URL syntax, s...	
EulerOS-SA-2024-1139 glibc security update	1	CVE-2023-4813	Feb 29, 2024 00:01:10 GMT+...	The glibc package contains standard libraries which are used by ...	Fix Ignore More

  b. In the dialog box displayed, click **OK**.

- Whitelisting one or more servers that are affected by a vulnerability

  HSS will ignore the vulnerability when scanning for vulnerabilities on these servers.

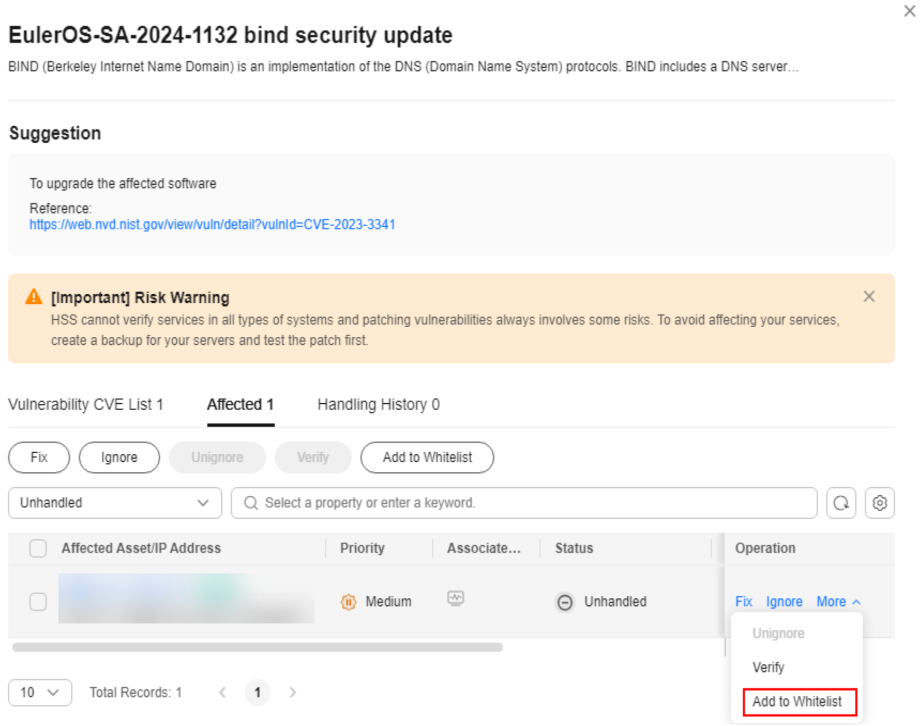
  a. Click a target vulnerability name.

  b. On the slide-out panel displayed, click the **Affected** tab.

  c. In the **Operation** column of the row containing the target server, click **More** and select **Add to Whitelist**.

You can also select multiple servers and click **Add to Whitelist** above the server list.

Figure 4-7 Whitelisting a single server that is affected by a vulnerability



EulerOS-SA-2024-1132 bind security update

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server...

Suggestion

To upgrade the affected software

Reference:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-3341

[Important] Risk Warning

HSS cannot verify services in all types of systems and patching vulnerabilities always involves some risks. To avoid affecting your services, create a backup for your servers and test the patch first.

Affected Asset/IP Address	Priority	Associate...	Status	Operation
[redacted]	Medium		Unhandled	Fix Ignore More

Total Records: 1

d. In the dialog box displayed, click **OK**.

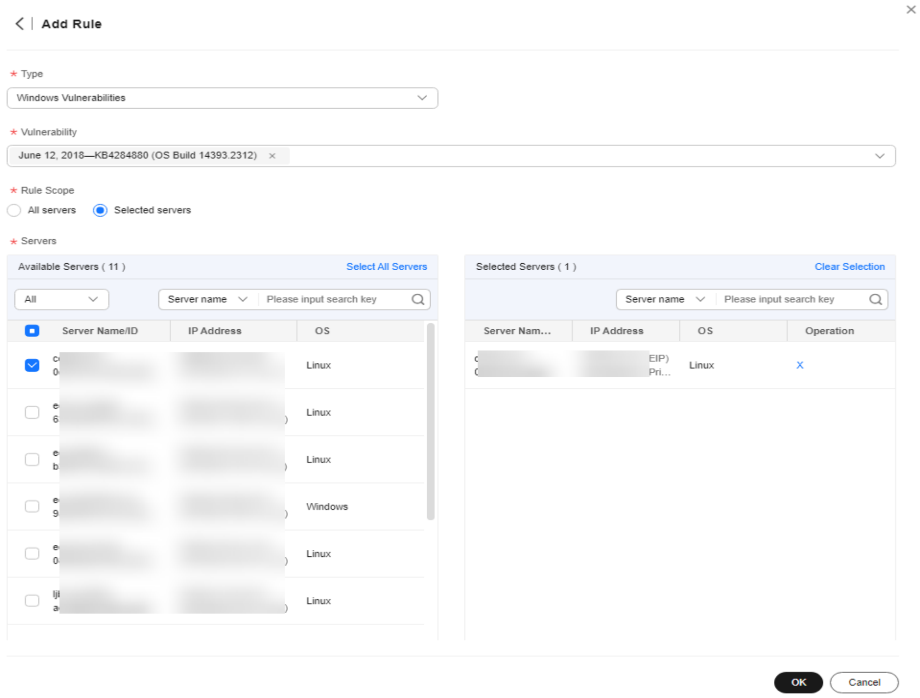
- Whitelisting vulnerabilities using whitelist rules

  a. In the upper right corner of the **Vulnerabilities** page, click **Configure Policy**. The **Configure Policy** slide-out panel is displayed.

  b. In the **Vulnerability Whitelist** area, click **Add Rule**.

  c. Configure a whitelist rule according to **Table 4-9**.

Figure 4-8 Configuring a whitelist rule



* Type: Windows Vulnerabilities

* Vulnerability: June 12, 2018—KB4284880 (OS Build 14393.2312)

* Rule Scope: ○ All servers ● Selected servers

* Servers

Available Servers (11)

☐	Server Name/ID	IP Address	OS
☑			Linux
☐			Linux
☐			Linux
☐			Windows
☐			Linux
☐			Linux

Selected Servers (1)

Server Nam...	IP Address	OS	Operation
	EIP) Pri...	Linux	X

Table 4-9 Vulnerability whitelist rule parameters

Parameter	Description
Type	Select the type of vulnerabilities to be whitelisted. Possible values are as follows: ■ **Linux Vulnerabilities** ■ **Windows Vulnerabilities** ■ **Web-CMS Vulnerabilities** ■ **Application Vulnerabilities** ■ **Emergency Vulnerabilities**
Vulnerability	Select one or more vulnerabilities to be whitelisted.

Parameter	Description
Rule Scope	Select the servers affected by the vulnerabilities. Possible values are as follows: ▪ **All servers** HSS will ignore the vulnerability when scanning for vulnerabilities on all servers. ▪ **Selected servers** Select one or more target servers. HSS will ignore the vulnerabilities when scanning for vulnerabilities on these servers. You can search for a target server by server name, ID, EIP, or private IP address.
Remarks (Optional)	Enter the remarks.

d. Click **OK**.

----End

Verifying the Vulnerability Fix

After you manually fix vulnerabilities, you are advised to verify the fixing result.

- **Method 1**: On the vulnerability details page, click **Verify** to perform one-click verification.

  NOTE

  - The fixing of emergency vulnerabilities cannot be verified.
  - Only application vulnerabilities of the JAR package can be verified. Application vulnerabilities of the non-JAR package are automatically filtered out and not verified.

- **Method 2**: Ensure the software has been upgraded to the latest version. The following table provides the commands to check the software upgrade result.

Table 4-10 Verification commands

OS	Verification Command
CentOS/Fedora /Euler/ Redhat/Oracle	rpm -qa | grep *Software_name*
Debian/Ubuntu	dpkg -l | grep *Software_name*
Gentoo	emerge --search *Software_name*

- **Method 3**: **Manually check for vulnerabilities** and view the vulnerability fixing results.

4.1.6 Managing the Vulnerability Whitelist

If you evaluate that some vulnerabilities do not affect your services and do not want to view the vulnerabilities in the vulnerability list, you can whitelist the vulnerabilities. After they are whitelisted, the vulnerabilities will be ignored in the vulnerability list and no alarms will be reported. The vulnerabilities will not be scanned and the vulnerability information will not be displayed when the next vulnerability scan task is executed.

This section describes how to whitelist a vulnerability, modify a vulnerability whitelist rule, and remove a vulnerability whitelist rule from the vulnerability whitelist.

Constraints

The basic edition does not support this function. For details about how to buy and upgrade HSS, see **Purchasing Quota** and **Upgrading Protection Quotas**.

Whitelisting 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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

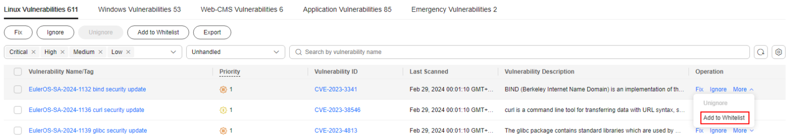
- Whitelisting all servers that are affected by a vulnerability

  HSS will ignore the vulnerability when scanning for vulnerabilities on all servers.

  a. In the **Operation** column of the row containing the target vulnerability, click **More** and select **Add to Whitelist**.

     You can also select multiple vulnerabilities and click **Add to Whitelist** above the vulnerability list.

     Figure 4-9 Whitelisting all servers that are affected by a vulnerability

     
Linux Vulnerabilities 611
Windows Vulnerabilities 53
Web-CMS Vulnerabilities 6
Application Vulnerabilities 85
Emergency Vulnerabilities 2
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical ×
High ×
Medium ×
Low ×
Unhandled
Search by vulnerability name
Unignore
Add to Whitelist

Vulnerability Name/Tag	Priority	Vulnerability ID	Last Scanned	Vulnerability Description	Operation
EulerOS-SA-2024-1132 bind security update	1	CVE-2023-3341	Feb 29, 2024 00:01:10 GMT+...	BIND (Berkeley Internet Name Domain) is an implementation of th...	Fix Ignore More
EulerOS-SA-2024-1136 curl security update	1	CVE-2023-38546	Feb 29, 2024 00:01:10 GMT+...	curl is a command line tool for transferring data with URL syntax, s...	
EulerOS-SA-2024-1139 glibc security update	1	CVE-2023-4813	Feb 29, 2024 00:01:10 GMT+...	The glibc package contains standard libraries which are used by ...	Fix Ignore More

  b. In the dialog box displayed, click **OK**.

- Whitelisting one or more servers that are affected by a vulnerability

  HSS will ignore the vulnerability when scanning for vulnerabilities on these servers.

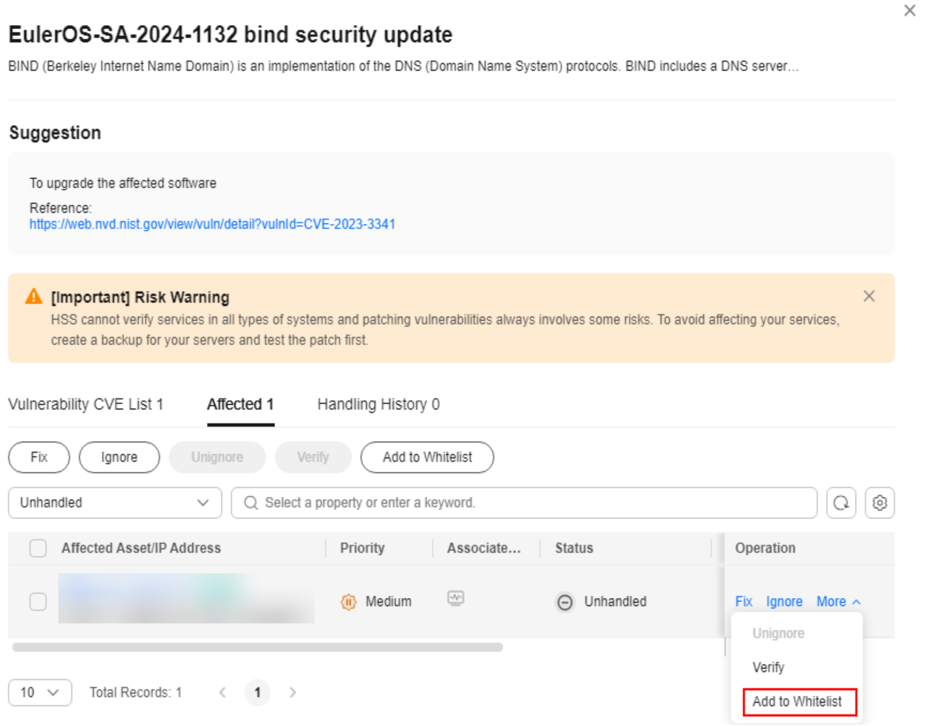
  a. Click a target vulnerability name.

  b. On the slide-out panel displayed, click the **Affected** tab.

  c. In the **Operation** column of the row containing the target server, click **More** and select **Add to Whitelist**.

     You can also select multiple servers and click **Add to Whitelist** above the server list.

Figure 4-10 Whitelisting a single server that is affected by a vulnerability



EulerOS-SA-2024-1132 bind security update

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server...

Suggestion

To upgrade the affected software

Reference:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-3341

[Important] Risk Warning

HSS cannot verify services in all types of systems and patching vulnerabilities always involves some risks. To avoid affecting your services, create a backup for your servers and test the patch first.

□ Affected Asset/IP Address	Priority	Associate...	Status	Operation
□ [redacted]	Medium		Unhandled	Fix Ignore More

d. In the dialog box displayed, click **OK**.

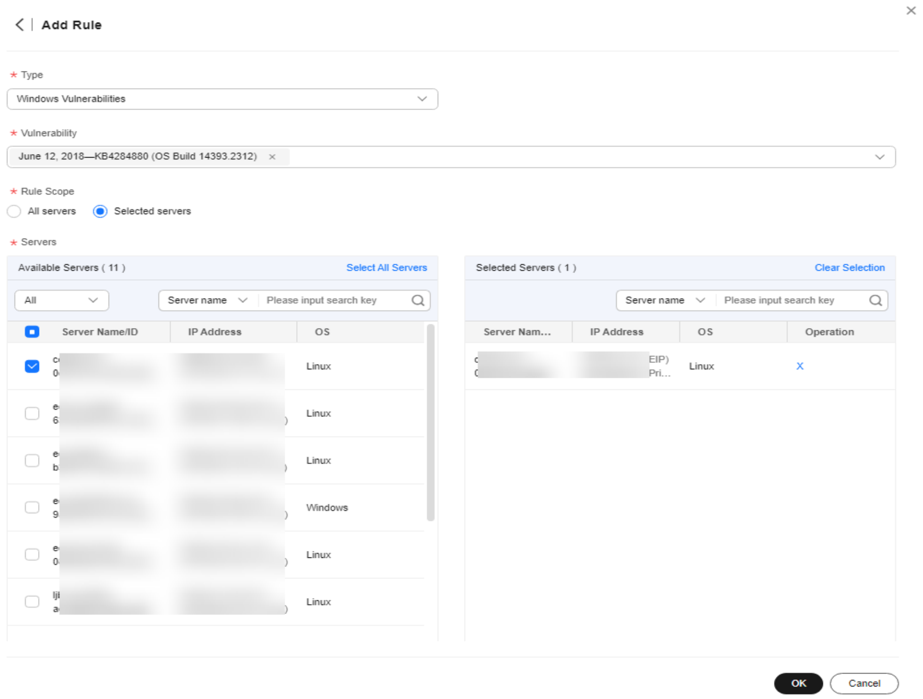
- Whitelisting vulnerabilities using whitelist rules

  a. In the upper right corner of the **Vulnerabilities** page, click **Configure Policy**. The **Configure Policy** slide-out panel is displayed.

  b. In the **Vulnerability Whitelist** area, click **Add Rule**.

  c. Configure a whitelist rule according to **Table 4-11**.

Figure 4-11 Configuring a whitelist rule



Add Rule

* Type

Windows Vulnerabilities

* Vulnerability

June 12, 2018—KB4284880 (OS Build 14393.2312) ×

* Rule Scope

○ All servers ● Selected servers

* Servers

Available Servers (11) Select All Servers

All | Server name | Please input search key

☑	Server Name/ID	IP Address	OS
☑	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Windows
□	[redacted]	[redacted]	Linux
□	[redacted]	[redacted]	Linux

Selected Servers (1) Clear Selection

Server name | Please input search key

Server Nam...	IP Address	OS	Operation
[redacted]	[redacted] EIP) Pri...	Linux	X

Table 4-11 Vulnerability whitelist rule parameters

Parameter	Description
Type	Select the type of vulnerabilities to be whitelisted. Possible values are as follows: ■ **Linux Vulnerabilities** ■ **Windows Vulnerabilities** ■ **Web-CMS Vulnerabilities** ■ **Application Vulnerabilities** ■ **Emergency Vulnerabilities**
Vulnerability	Select one or more vulnerabilities to be whitelisted.

Parameter	Description
Rule Scope	Select the servers affected by the vulnerabilities. Possible values are as follows: ▪ **All servers** HSS will ignore the vulnerability when scanning for vulnerabilities on all servers. ▪ **Selected servers** Select one or more target servers. HSS will ignore the vulnerabilities when scanning for vulnerabilities on these servers. You can search for a target server by server name, ID, EIP, or private IP address.
Remarks (Optional)	Enter the remarks.

d. Click **OK**.

----End

Editing a Vulnerability 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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 In the upper right corner of the **Vulnerabilities** page, click **Configure Policy**. The **Configure Policy** slide-out panel is displayed.

Step 5 In the row containing the desired vulnerability whitelist rule, click **Edit** in the **Operation** column.

Step 6 On the editing page, modify the information and click **OK**.

----End

Removing a Vulnerability Whitelist Rule from the Vulnerability 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** > **HSS**.

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 In the upper right corner of the **Vulnerabilities** page, click **Configure Policy**. The **Configure Policy** slide-out panel is displayed.

Step 5 In the row containing the desired vulnerability whitelist rule, click **Delete** in the **Operation** column.

Step 6 In the dialog box displayed, confirm the information and click **OK**.

----End

4.1.7 Viewing Vulnerability Handling History

For vulnerabilities that have been handled, you can refer to this section to view the vulnerability handling history (handler and handling time).

Constraints

The basic edition does not support this function. For details about how to buy and upgrade HSS, see **Purchasing Quota** and **Upgrading Protection Quotas**.

Viewing the Handling History of a Vulnerability

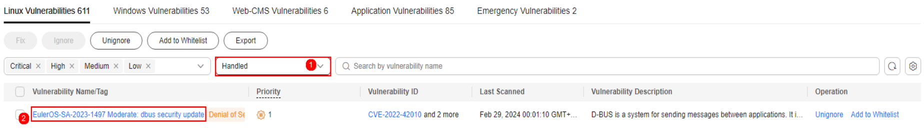
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 In the list of handled vulnerabilities, click a vulnerability name. The vulnerability details slide-out panel is displayed.

Figure 4-12 Selecting Handled from the drop-down list


Linux Vulnerabilities 611
Windows Vulnerabilities 53
Web-CMS Vulnerabilities 6
Application Vulnerabilities 85
Emergency Vulnerabilities 2
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical ×
High ×
Medium ×
Low ×
1
2

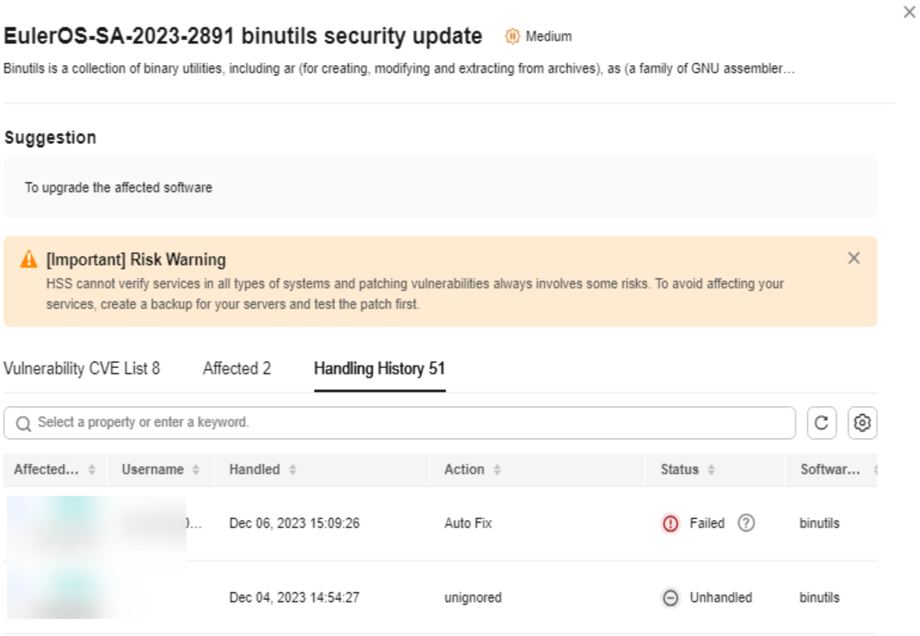
Handled

Search by vulnerability name

Vulnerability Name/Tag	Priority	Vulnerability ID	Last Scanned	Vulnerability Description	Operation
EulerOS-SA-2023-1497 Moderate: dbus security update Denial of Se	1	CVE-2022-42010 and 2 more	Feb 29, 2024 00:01:10 GMT+...	D-BUS is a system for sending messages between applications. It i...	Unignore Add to Whitelist

Step 5 Click the **Handling History** tab to view the handling history of the vulnerability.

Figure 4-13 Handling history



EulerOS-SA-2023-2891 binutils security update Medium

Binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assembler...

Suggestion

To upgrade the affected software

[Important] Risk Warning
HSS cannot verify services in all types of systems and patching vulnerabilities always involves some risks. To avoid affecting your services, create a backup for your servers and test the patch first.

Vulnerability CVE List 8 | Affected 2 | **Handling History 51**

Select a property or enter a keyword.

Affected...	Username	Handled	Action	Status	Softwar...
[redacted]	[redacted]	Dec 06, 2023 15:09:26	Auto Fix	Failed	binutils
[redacted]		Dec 04, 2023 14:54:27	unignored	Unhandled	binutils

----End

Viewing the Handling History of all 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Security Operations** > **Handling History**. The **Handling History** page is displayed.

Step 4 On the **Vulnerabilities** tab page displayed, view the handling history of all vulnerabilities.

- Viewing the vulnerability handling history of a specified enterprise project

  In the upper left corner of the **Handling History** page, select an enterprise project for **Enterprise Project** to view the handling history of server vulnerabilities in the enterprise project.

- Viewing the vulnerability handling history of a specified property

  In the search box above the vulnerability handling history list, enter a vulnerability type, vulnerability name, or server IP address, and click 🔍 to view the vulnerability handling history of a specified property.

----End

4.2 Baseline Inspection

4.2.1 Baseline Inspection Overview

Baseline Inspection includes password complexity policy detection, common weak password detection, and configuration check. It can detect insecure password configurations and risky configurations in key software on servers, and provide **rectification suggestions** for detected risks, helping you correctly handle risky configurations on servers.

Baseline Inspection Content

Item	Description	Supported Check Mode	Supported HSS Version
Unsafe configuration	Check the unsafe Tomcat, Nginx, SSH login, and system configurations found by HSS. Currently, the following check standards and types are supported: ● For Linux, – Cloud security practices: Apache2, Docker, MongoDB, Redis, MySQL5, Nginx, Tomcat, SSH, vsftp, CentOS7, EulerOS, EulerOS_ext, Kubernetes-Node, Kubernetes-Master, MySQL5.7, Nginx1.17, Redis6.2, Apache2.4, Kafka, ZooKeeper3.6, GaussDB, Tomcat8, Tomcat9, HCE1.1 and HCE2.0. – DJCP MLPS compliance: Apache 2, MongoDB, MySQL 5, Nginx, Tomcat, CentOS 6, CentOS 7, CentOS 8, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, Alma, SUSE 12, SUSE 15, and HCE1.1 ● For Windows, The cloud security practice baseline can check MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008, Windows_2012, Windows_2016, Windows_2019, and SqlServer.	● Automated baseline checks ● Manual baseline checks	Enterprise, premium, WTP, and container edition
Password complexity policies	Check whether your password complexity policy of Linux system account is proper and modify it based on suggestions provided by HSS, improving password security.	Manual baseline checks	All versions

Item	Description	Supported Check Mode	Supported HSS Version
Common weak passwords	Weak passwords defined in the common weak password library. You can check for accounts and remind users to change them. Linux supports weak password detection for MySQL, FTP, and system accounts. Windows supports weak password detection for system accounts.	● Automated baseline checks ● Manually Performing a Baseline Check	All

Usage Process

Table 4-12 Usage process

No.	Operation	Description
1	**Performing baseline inspection**	The baseline inspection supports automatic and manual baseline checks. ● Automatic baseline check: HSS automatically performs a check for all server configurations and common weak passwords **at 01:00 every day**. Premium edition, web tamper protection edition, and container edition allow you to customize the automatic detection period for configurations and common weak passwords. For details, see **Configuration Check** and **Weak Password Scan**. ● Manual baseline inspection: To view the real-time baseline risks of a specified server, you can manually perform a baseline inspection.
2	**Viewing and processing baseline inspection results**	After the baseline inspection is complete, you need to view and handle baseline configuration risks.

4.2.2 Performing Baseline Inspection

The baseline check supports automatic and manual baseline checks.

- Automatic baseline check: checks server configurations and common weak passwords.
- Manual baseline check: To view the real-time baseline risks of a specified server or detect the password complexity policy, you can manually perform a baseline check.

Automated Baseline Checks

HSS automatically performs a check for all server configurations and common weak passwords at **01:00 every day**.

Premium edition, web tamper protection edition, and container edition allow you to customize the automatic detection period for configurations and common weak passwords. For details, see Configuration Check and Weak Password Scan.

Manually Performing a Baseline Check

Step 1 Log in to the management console.

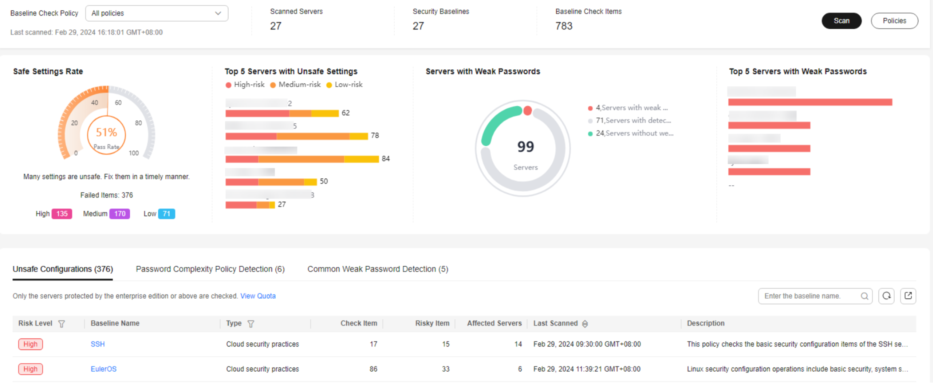
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 4-14 Baseline check overview



Baseline Check Policy: All policies
Last scanned: Feb 29, 2024 16:18:01 GMT+08:00
Scanned Servers: 27
Security Baselines: 27
Baseline Check Items: 783

Scan
Policies
Safe Settings Rate
0
20
40
60
80
100
51%
Pass Rate
Many settings are unsafe. Fix them in a timely manner.
Failed Items: 376
High 135
Medium 170
Low 71
Top 5 Servers with Unsafe Settings
High-risk
Medium-risk
Low-risk
62
78
84
50
27
Servers with Weak Passwords
99
Servers
4,Servers with weak ...
71,Servers with detec...
24,Servers without we...
Top 5 Servers with Weak Passwords
--
Unsafe Configurations (376)
Password Complexity Policy Detection (6)
Common Weak Password Detection (5)
Enter the baseline name.

Only the servers protected by the enterprise edition or above are checked. View Quota

Risk Level	Baseline Name	Type	Check Item	Risky Item	Affected Servers	Last Scanned	Description
High	SSH	Cloud security practices	17	15	14	Feb 29, 2024 09:30:00 GMT+08:00	This policy checks the basic security configuration items of the SSH se...
High	EulerOS	Cloud security practices	86	33	6	Feb 29, 2024 11:39:21 GMT+08:00	Linux security configuration operations include basic security, system s...

Step 4 (Optional) Create a manual baseline check policy.

Before manually checking the baseline policy, you need to create a manual baseline check policy for the target server. If you have created a policy for the target server, skip this step.

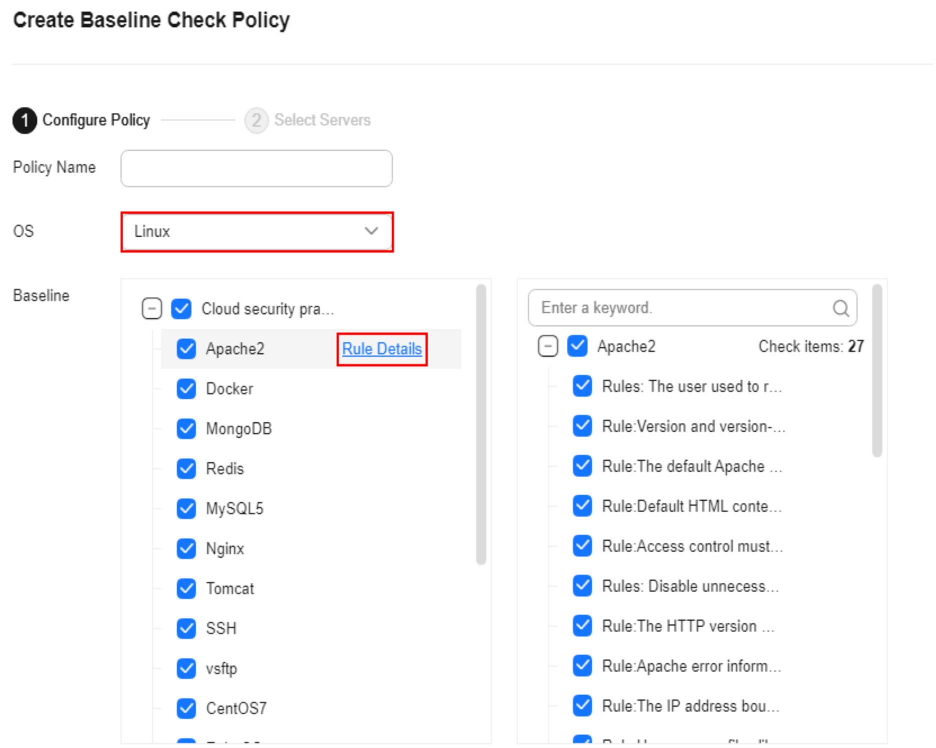
1. Click **Policies** in the upper right corner of the page.
2. Click **Create Policy** and configure the policy information by referring to Table 4-13.

   To check baseline details, click **Rule Details** on the right of a baseline name.

   NOTE

   If you select **Linux** for **OS**, you can select any checks included in **Baseline** and edit rules. This function is not supported for Windows servers.

Figure 4-15 Creating a policy



Create Baseline Check Policy

1 Configure Policy — 2 Select Servers

Policy Name

OS: Linux

Baseline

☑ Cloud security pra...
- ☑ Apache2 Rule Details
- ☑ Docker
- ☑ MongoDB
- ☑ Redis
- ☑ MySQL5
- ☑ Nginx
- ☑ Tomcat
- ☑ SSH
- ☑ vsftp
- ☑ CentOS7

Enter a keyword.

☑ Apache2 Check items: 27
- ☑ Rules: The user used to r...
- ☑ Rule:Version and version-...
- ☑ Rule:The default Apache ...
- ☑ Rule:Default HTML conte...
- ☑ Rule:Access control must...
- ☑ Rules: Disable unnecess...
- ☑ Rule:The HTTP version ...
- ☑ Rule:Apache error inform...
- ☑ Rule:The IP address bou...

Table 4-13 Baseline policy parameters

Parameter	Description	Example Value
Policy	Policy name	linux_web1_security_policy
OS	OS that will be checked. – Linux – Windows	Linux

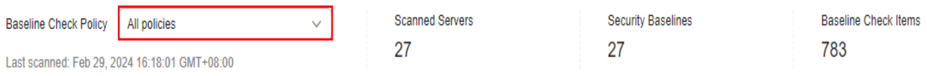
Parameter	Description	Example Value
Baseline	Baseline used for a check. Check items are as follows: – For Linux, ■ Cloud security practices: Apache2, Docker, MongoDB, Redis, MySQL5, Nginx, Tomcat, SSH, vsftp, CentOS7, EulerOS, EulerOS_ext, Kubernetes-Node, Kubernetes-Master, MySQL5.7, Nginx1.17, Redis6.2, Apache2.4, Kafka, ZooKeeper3.6, GaussDB, Tomcat8, Tomcat9, HCE1.1 and HCE2.0. ■ DJCP MLPS compliance: Apache 2, MongoDB, MySQL 5, Nginx, Tomcat, CentOS 6, CentOS 7, CentOS 8, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, Alma, SUSE 12, SUSE 15, and HCE1.1 – For Windows, The cloud security practice baseline can check MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008, Windows_2012, Windows_2016, Windows_2019, and SqlServer.	**Cloud security practices**: Select all. **DJCP MLPS**: Select all.

3. Confirm the information, click **Next**, and select the server to be associated with the application based on the server name, server ID, EIP, or private IP address.

4. Confirm the information and click **OK**. The baseline policy will be displayed in the policy list.

Step 5 In the upper left corner of the **Baseline Inspection** page, select the target baseline inspection policy.

Figure 4-16 Selecting the target baseline policy



Baseline Check Policy: All policies
Last scanned: Feb 29, 2024 16:18:01 GMT+08:00
Scanned Servers 27
Security Baselines 27
Baseline Check Items 783

Step 6 Click **Scan** in the upper right corner of the page.

Step 7 If the time displayed in the **Last scanned** area under the **Baseline Check Policy** is the actual check time, the check is complete.

NOTE

- After a manual check is performed, the button will display **Scanning** and be disabled. If the check time exceeds 30 minutes, the button will be automatically enabled again. If the time displayed in the **Last scanned** area becomes the current check time, it indicates the check has completed.
- After the check is complete, you can view the check results and handling suggestions by referring to **Viewing and Processing Baseline Check Results**.

----End

4.2.3 Viewing and Processing Baseline Check Results

This topic provides suggestions on how to fix baseline configuration risks on the server.

Constraints

Only enterprise edition, premium edition, web tamper protection edition, and container edition are supported.

Detection Description

The MySQL baseline detection of Linux OS is based on the MySQL 5 security configuration specifications. If MySQL 8 is installed on your server, the following check items are not displayed in the detection results, because they are discarded in that version. The detection results are displayed only on the server whose MySQL version is 5.

- Rule: Do not set **old_passwords** to **1**.
- Rule: Set secure_auth to **1** or **ON**.
- Rule: Do not set **skip_secure_auth**.
- Rule: Set **log_warnings** to **2**.
- Rule: Configure the MySQL binlog clearing policy.
- Rule: The **sql_mode** parameter contains **NO_AUTO_CREATE_USER**.
- Rule: Use the MySQL audit plug-in.

Viewing Baseline Check Overview 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

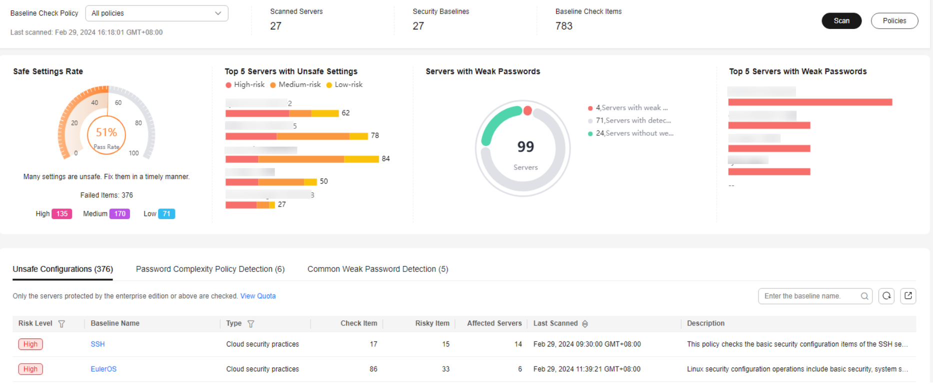
NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click different tabs on the displayed page to check detected unsafe configurations. **Figure 1** lists the corresponding parameters.

To view the check results of servers under different manual baseline check policies, you can switch between baseline check policies.

Figure 4-17 Baseline check overview



Baseline Check Policy: All policies

Last scanned: Feb 29, 2024 16:18:01 GMT+08:00

Scanned Servers: 27

Security Baselines: 27

Baseline Check Items: 783

Many settings are unsafe. Fix them in a timely manner.

Failed Items: 376

High 135 Medium 170 Low 71

Only the servers protected by the enterprise edition or above are checked. View Quota

Risk Level	Baseline Name	Type	Check Item	Risky Item	Affected Servers	Last Scanned	Description
High	SSH	Cloud security practices	17	15	14	Feb 29, 2024 09:30:00 GMT+08:00	This policy checks the basic security configuration items of the SSH se...
High	EulerOS	Cloud security practices	86	33	6	Feb 29, 2024 11:39:21 GMT+08:00	Linux security configuration operations include basic security, system s...

Table 4-14 Baseline check overview

Parameter	Description
Baseline check policy	Available baseline check policies that have been added. You can select, create, edit, and delete these policies.
Scanned servers	Total number of detected servers.
Security baselines	Number of baselines executed during the server detection.
Baseline check items	Total number of checked server configuration items.
Safe settings rate	Percentage of configuration items that passed the baseline check to the total number of check items. Failed items are displayed by risk level.
Top 5 servers with unsafe settings	Statistics on servers with server configuration risks. The top 5 servers with the highest risks are preferentially sorted. If no high-risk settings exist, the servers are sorted into medium-risk and low-risk ones in sequence.
Servers with weak passwords	Total number of detected servers, as well as the numbers of servers with weak passwords, those without weak passwords, and those with weak password detection disabled.
Top 5 servers with weak passwords	Statistics on the top 5 servers with most weak password risks.
Unsafe configuration	Alarms generated for servers with configuration risks and the risk statistics.
Password complexity policies	Statistics on servers with weak passwords that do not meet the baseline requirements.

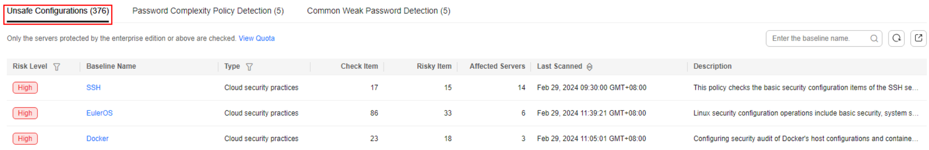
Parameter	Description
Common weak passwords	Statistics on servers with weak passwords and accounts.

----End

Viewing and Processing Configuration Check Results

Step 1 Click the **Unsafe Configurations** tab to view the risk items. For more information, see **Table 4-15**.

Figure 4-18 Viewing unsafe configuration details



Unsafe Configurations (376)
Password Complexity Policy Detection (5)
Common Weak Password Detection (5)
Enter the baseline name.

Only the servers protected by the enterprise edition or above are checked. View Quota

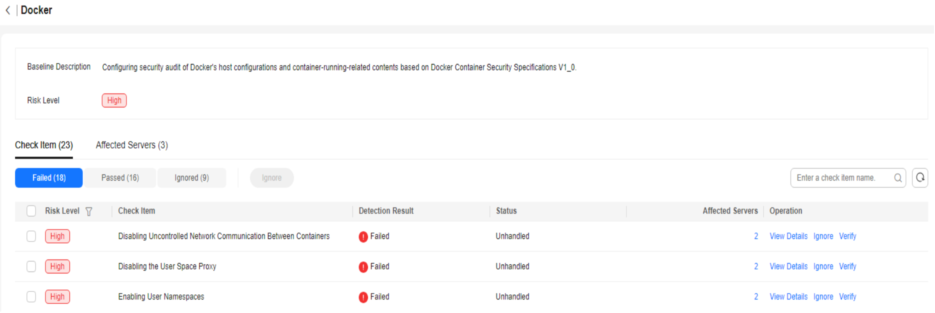
Risk Level	Baseline Name	Type	Check Item	Risky Item	Affected Servers	Last Scanned	Description
High	SSH	Cloud security practices	17	15	14	Feb 29, 2024 09:30:00 GMT+08:00	This policy checks the basic security configuration items of the SSH se...
High	EulerOS	Cloud security practices	86	33	6	Feb 29, 2024 11:39:21 GMT+08:00	Linux security configuration operations include basic security, system s...
High	Docker	Cloud security practices	23	18	3	Feb 29, 2024 11:05:01 GMT+08:00	Configuring security audit of Docker's host configurations and containe...

Table 4-15 Parameter description

Parameter	Description
Risk level	Level of a detection result. ● High ● Low ● Medium ● Secure
Baseline name	Name of the baseline that is checked.
Type	Policy type of the baseline that has been checked. ● Cloud security practices ● DJCP MLPS
Check item	Total number of configuration items that are checked.
Risky item	Total number of the risky configurations.
Affected servers	Total number of servers affected by the detected risks in a baseline.
Last scanned	Time when the last detection was performed.
Description	Description of a baseline.

Step 2 Click the target baseline name in the list to view the baseline description, affected servers, and details about all check items.

Figure 4-19 Viewing baseline check details



Docker

Baseline Description Configuring security audit of Docker's host configurations and container-running-related contents based on Docker Container Security Specifications V1_0.

Risk Level High

Check Item (23) Affected Servers (3)

Failed (18) Passed (16) Ignored (9) Ignore

Enter a check item name.

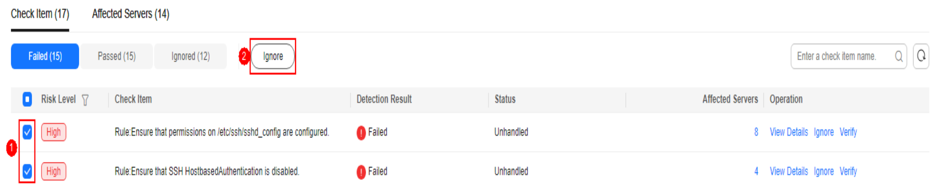
	Risk Level	Check Item	Detection Result	Status	Affected Servers	Operation
□	High	Disabling Uncontrolled Network Communication Between Containers	Failed	Unhandled	2	View Details Ignore Verify
□	High	Disabling the User Space Proxy	Failed	Unhandled	2	View Details Ignore Verify
□	High	Enabling User Namespaces	Failed	Unhandled	2	View Details Ignore Verify

Step 3 Handle risk items.

- **Ignoring risks**

  Click **Ignore** in the **Operation** column of the target check item to ignore a check item. Select multiple check items and click **Ignore** to ignore them in batches.

  Figure 4-20 Ignoring risks

  Check Item (17) Affected Servers (14)

  Failed (15) Passed (15) Ignored (12) 2 Ignore

  Enter a check item name.

	Risk Level	Check Item	Detection Result	Status	Affected Servers	Operation
☑	High	Rule:Ensure that permissions on /etc/ssh/sshd_config are configured.	Failed	Unhandled	8	View Details Ignore Verify
☑	High	Rule:Ensure that SSH HostbasedAuthentication is disabled.	Failed	Unhandled	4	View Details Ignore Verify

- **Fixing risks**

  a. Click **View Details** in the **Operation** column of the target risk item to view the check item details.

  b. View the content in the **Audit Description**, **Suggestion**, and **Affected Servers**. Rectify the unsafe configurations.

  NOTE

  ■ Currently, one-click fixing is supported for some EulerOS baseline configurations and CentOS 8 baseline configurations. You can simply click **Fix** in the **Operation** column of the target EulerOS or CentOS check item to fix the unsafe configurations. If some parameters need to be configured during restoration, retain the default values.

  ■ You are advised to fix the settings with high severity immediately and fix those with medium or low severity.

  c. After the repair is complete, click **Verify** on the **Affected Servers** tab page to verify the result.

  If a failed check item has been fixed, you can update its status through verification.

NOTE

- Currently, baseline checks are not supported for Windows OSs.
- The agent status of the target server must be online.
- Only one risk item can be verified at a time. Other risk items can be verified only after the risk items are verified.
- Baseline checks are supported for the following Linux OSs: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 6, CentOS 7, CentOS 8, EulerOS, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, Suse 12, Suse 15, HCE1.1, and HCE2.0.

d. Click **Verify**.

e. Return to the check item list page and view the status of the risk item.

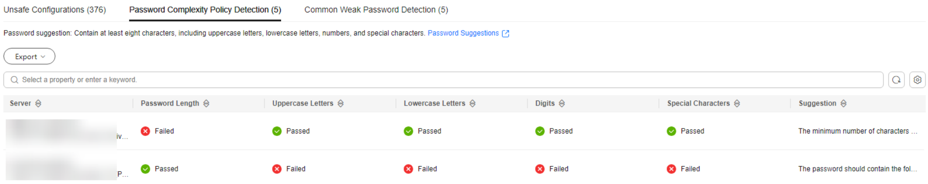
The status changes to **Verifying**. The system starts automatic verification. After the verification is complete, check the status. If a check item failed to be fixed, click **View Cause** to view the cause. Then, fix it again.

----End

Viewing and Processing the Password Complexity Policy Detection Result

Step 1 Click the **Password Complexity Policy Detection** tab to view the risk statistical items and handling suggestions. For more information, see **Table 4-16**.

Figure 4-21 Viewing password complexity policy detection details



Unsafe Configurations (376)
Password Complexity Policy Detection (5)
Common Weak Password Detection (5)

Password suggestion: Contain at least eight characters, including uppercase letters, lowercase letters, numbers, and special characters. Password Suggestions

Export
Select a property or enter a keyword.

Server	Password Length	Uppercase Letters	Lowercase Letters	Digits	Special Characters	Suggestion
[redacted] iv...	Failed	Passed	Passed	Passed	Passed	The minimum number of characters ...
[redacted] P...	Passed	Failed	Failed	Failed	Failed	The password should contain the fol...

Table 4-16 Parameter description

Parameter	Description
Server	Name and public/private IP address of the detected server.
Password length	Whether the password length of the target server meets the requirements. ● Passed ● Failed
Uppercase letters	Whether the uppercase letters used in the target server password meet the requirements. ● Passed ● Failed

Parameter	Description
Lowercase letters	Whether the lowercase letters used in the target server password meet the requirements. ● Passed ● Failed
Digits	Whether the digits used in the target server password meet the requirements. ● Passed ● Failed
Special characters	Whether the special characters used in the target server password meet the requirements. ● Passed ● Failed
Suggestion	Suggestion for fixing unsafe passwords

Step 2 Modify the password complexity policy on the server as recommended.

- 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 server, see **How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS?**
- For details about how to modify the password complexity policy on a Windows server, see **How Do I Set a Secure Password Complexity Policy in a Windows OS?**

Step 3 After modifying the password complexity policy, perform a manual check in the upper part of the **Baseline Checks** page to verify the result.

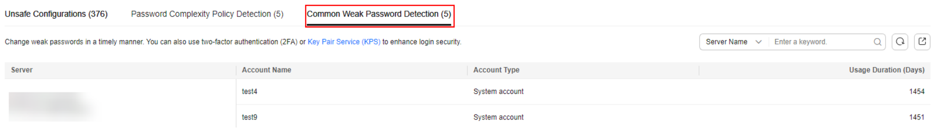
If you do not perform a manual verification, HSS will automatically check the settings at 00:00:00 the next day.

----End

Viewing and Processing Common Weak Password Detection Results

Step 1 Click the Common Weak Password Detection tab to view the statistics of risky weak password accounts on the server. For more information, see **Viewing common weak password detection**.

Figure 4-22 Viewing common weak password detection



Unsafe Configurations (376)
Password Complexity Policy Detection (5)
Common Weak Password Detection (5)
Server Name
Enter a keyword.

Change weak passwords in a timely manner. You can also use two-factor authentication (2FA) or Key Pair Service (KPS) to enhance login security.

Server	Account Name	Account Type	Usage Duration (Days)
[redacted]	test4	System account	1454
	test9	System account	1451

Table 4-17 Parameter description

Parameter	Description
Server	Name and public/private IP address of the detected server.
Account name	Accounts with weak passwords that are detected on the target server.
Account type	Type of an account.
Usage duration (Days)	Period for using a weak password.

Step 2 Log in to the server and change the weak password.

NOTE

- To enhance server security, you are advised to modify the accounts with weak passwords 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.
- A password should contain more than eight characters, including uppercase letters, lowercase letters, digits, and special characters.

Step 3 After the weak password is changed, perform a manual check in the upper part of the **Baseline Checks** page to verify the result.

If you do not perform a manual verification, HSS will automatically check the settings at 00:00:00 the next day.

----End

4.2.4 Exporting the Baseline Check Report

This section describes how to export a baseline check report.

Constraints

Only enterprise edition, premium edition, web tamper protection edition, and container edition are supported.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

Step 4 Perform the following operations to export the detection result based on the baseline check type:

- Unsafe configurations

Click the **Unsafe Configurations** tab and click in the upper right corner of the list to export the result.

You can click **Risk Level** and **Type** to filter and download alarm information.

- Password complexity policies

  Click the **Password Complexity Policy Detection** tab. In the upper left corner of the list, click **Export** > **Export all data to an XLSX file** to export the result.

- Common weak passwords

  Click the **Common Weak Password Detection** tab. In the upper right corner of the list, click to export the result.

  You can enter the server name, IP address, or account name in the upper right corner of the list, and click to search for the target content and download it.

----End

4.2.5 Managing Manual Baseline Check Policies

This section describes how to modify a created manual baseline check policy.

Editing a Manual Baseline Check Policy

Step 1 Log in to the management console.

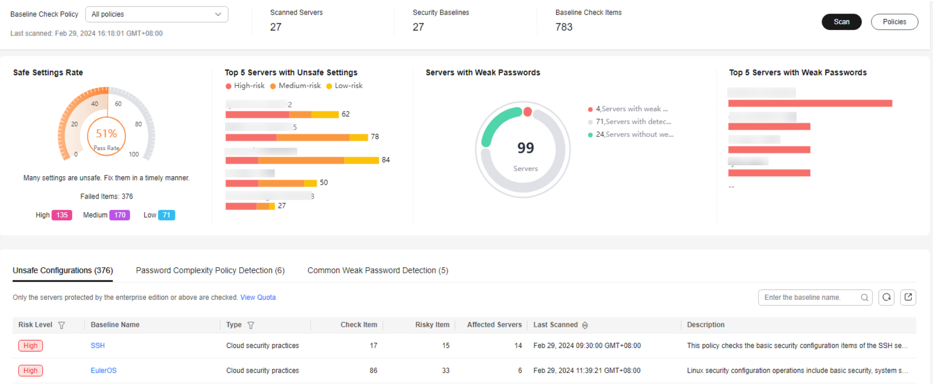
Step 2 In the upper left corner of the page, select a region, click , and choose **Security & Compliance** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 4-23 Baseline check overview



Baseline Check Policy: All policies

Last scanned: Feb 29, 2024 16:18:01 GMT+08:00

Scanned Servers: 27

Security Baselines: 27

Baseline Check Items: 783

Many settings are unsafe. Fix them in a timely manner.

Failed Items: 376

High 135 Medium 170 Low 71

Unsafe Configurations (376) | Password Complexity Policy Detection (6) | Common Weak Password Detection (5)

Only the servers protected by the enterprise edition or above are checked. View Quota

Risk Level	Baseline Name	Type	Check Item	Risky Item	Affected Servers	Last Scanned	Description
High	SSH	Cloud security practices	17	15	14	Feb 29, 2024 09:30:00 GMT+08:00	This policy checks the basic security configuration items of the SSH se...
High	EulerOS	Cloud security practices	86	33	6	Feb 29, 2024 11:39:21 GMT+08:00	Linux security configuration operations include basic security, system s...

Step 4 Click **Policies** in the upper right corner of the page.

Step 5 Click **Edit** in the **Operation** column of a policy. On the policy details page that is displayed, configure the policy name and check items.

NOTE

If you select **Linux** for **OS**, you can select any checks included in **Baseline** and edit rules. This function is not supported for Windows servers.

Step 6 Confirm the configuration, click **Next**, and select servers.

Step 7 Confirm the information and click **OK**. You can view the updated policy in the policy list.

----End

Deleting a Manual Baseline Check Policy

Step 1 Log in to the management console.

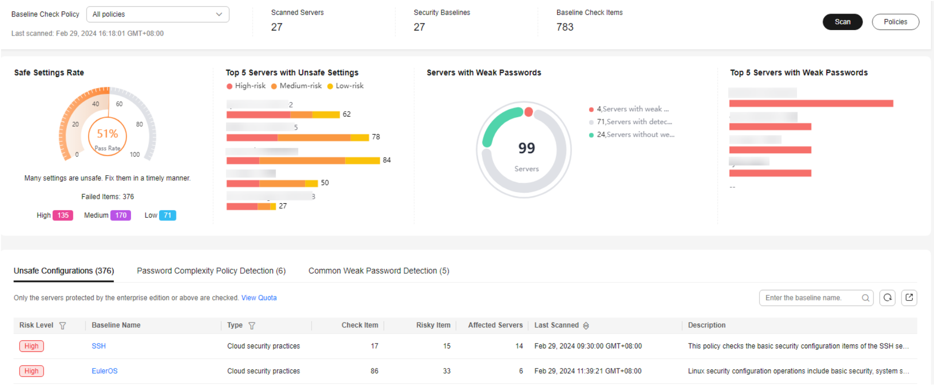
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 4-24 Baseline check overview



Baseline Check Policy: All policies
Last scanned: Feb 29, 2024 16:18:01 GMT+08:00

Scanned Servers: 27
Security Baselines: 27
Baseline Check Items: 783

Scan
Policies
Safe Settings Rate
0
20
40
60
80
100
51%
Pass Rate
Top 5 Servers with Unsafe Settings
High-risk
Medium-risk
Low-risk
2
62
5
78
84
50
3
27
Servers with Weak Passwords
99
Servers
4,Servers with weak ...
71,Servers with detec...
24,Servers without we...
Top 5 Servers with Weak Passwords
--

Many settings are unsafe. Fix them in a timely manner.

Failed Items: 376

High 135 Medium 170 Low 71

Unsafe Configurations (376)
Password Complexity Policy Detection (6)
Common Weak Password Detection (5)

Only the servers protected by the enterprise edition or above are checked. View Quota

Enter the baseline name.

Risk Level	Baseline Name	Type	Check Item	Risky Item	Affected Servers	Last Scanned	Description
High	SSH	Cloud security practices	17	15	14	Feb 29, 2024 09:30:00 GMT+08:00	This policy checks the basic security configuration items of the SSH se...
High	EulerOS	Cloud security practices	86	33	6	Feb 29, 2024 11:39:21 GMT+08:00	Linux security configuration operations include basic security, system s...

Step 4 Click **Policies** in the upper right corner of the page.

Step 5 Click **Delete** in the **Operation** column of a policy. In the dialog box that is displayed, confirm the information and click **OK**.

NOTE

Only user-defined policies can be deleted. Default policies **default_linux_security_check_policy** and **default_windows_security_check_policy** cannot be deleted.

----End

4.3 Container Image Security

4.3.1 SWR Image Repository Vulnerabilities

This section describes how to view SWR image repository vulnerabilities and fix the vulnerabilities as prompted.

Prerequisites

Container node protection has been enabled. For details, see **Enabling Container Protection**.

Detection Method

After you enable node protection, your Linux images will be scanned automatically.

Constraints

Only vulnerabilities in Linux images can be checked.

Procedures

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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Prediction** > **Container Images**.

Step 4 Click the **SWR Image Repository Vulnerability** tab to view the system and application vulnerability lists. For details about the vulnerability list, see **SWR image repository vulnerability parameters**

Table 4-18 SWR image repository vulnerability parameters

Parameter	Description
Vulnerability Name	You can click a vulnerability name to view basic information about a vulnerability and the images affected by the vulnerability.
Repair Urgency	You are advised to fix vulnerabilities of the high and medium levels.
Historically Affected Images	Images affected by the vulnerability.
Solution	HSS provides a recommended solution to the vulnerability. Click the solution description to go to the details page.

----End

4.3.2 Viewing Malicious File Detection Results

Malicious files in the private images can be automatically detected, helping you discover and eliminate the security threats in your assets.

Check Frequency

A comprehensive check is automatically performed in the early morning every day.

Prerequisites

Container protection has been enabled.

Constraints

Only malicious files in Linux images can be detected.

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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Prediction** > **Container Images**.

Step 4 Click the **Malicious Files** tab to view details about the malicious files in private images. Delete the malicious files or create images again as needed based on the scan result.

- Malicious files include Trojans, worms, viruses, and Adware.
- In the **Image Tag** column, click an image version to view its vulnerability report.

----End

5 Prevention

5.1 Application Protection

5.1.1 Enabling Application Protection

To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.

Technical Principles

Probes (monitoring and protection code) are added to the checkpoints (key functions) of applications through dynamic code injection. The probes identify attacks based on predefined rules, data passing through the checkpoints, and contexts (application logic, configurations, data, and event flows).

Prerequisites

You have enabled HSS premium, WTP, or container edition.

Constraints

- Currently, only Linux servers are supported.
- So far, only Java applications can be protected.
- The premium, WTP, and container editions support operations related to application protection.

Procedure

Step 1 Log in to the management console.

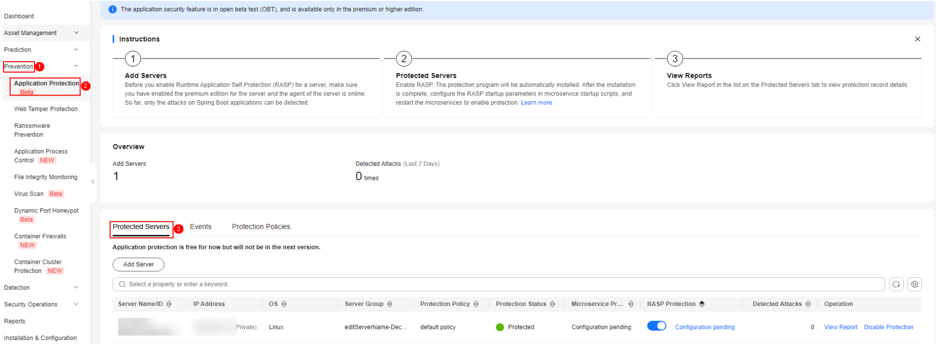
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Prevention** > **Application Protection**. Click the **Protected Servers** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-1 Viewing protection settings



The application security feature is in open beta test (OBT), and is available only in the premium or higher edition.

Instructions

1 Add Servers
Before you enable Runtime Application Self Protection (RASP) for a server, make sure you have enabled the premium edition for the server and the agent of the server is online. So far, only the attacks on Spring Boot applications can be detected.

2 Protected Servers
Enable RASP. The protection program will be automatically installed. After the installation is complete, configure the RASP startup parameters in microservice startup scripts, and restart the microservices to enable protection. Learn more

3 View Reports
Click View Report in the list on the Protected Servers tab to view protection record details.

Overview

Add Servers
1

Detected Attacks (Last 7 Days)
0 times

Application protection is free for now but will not be in the next version.

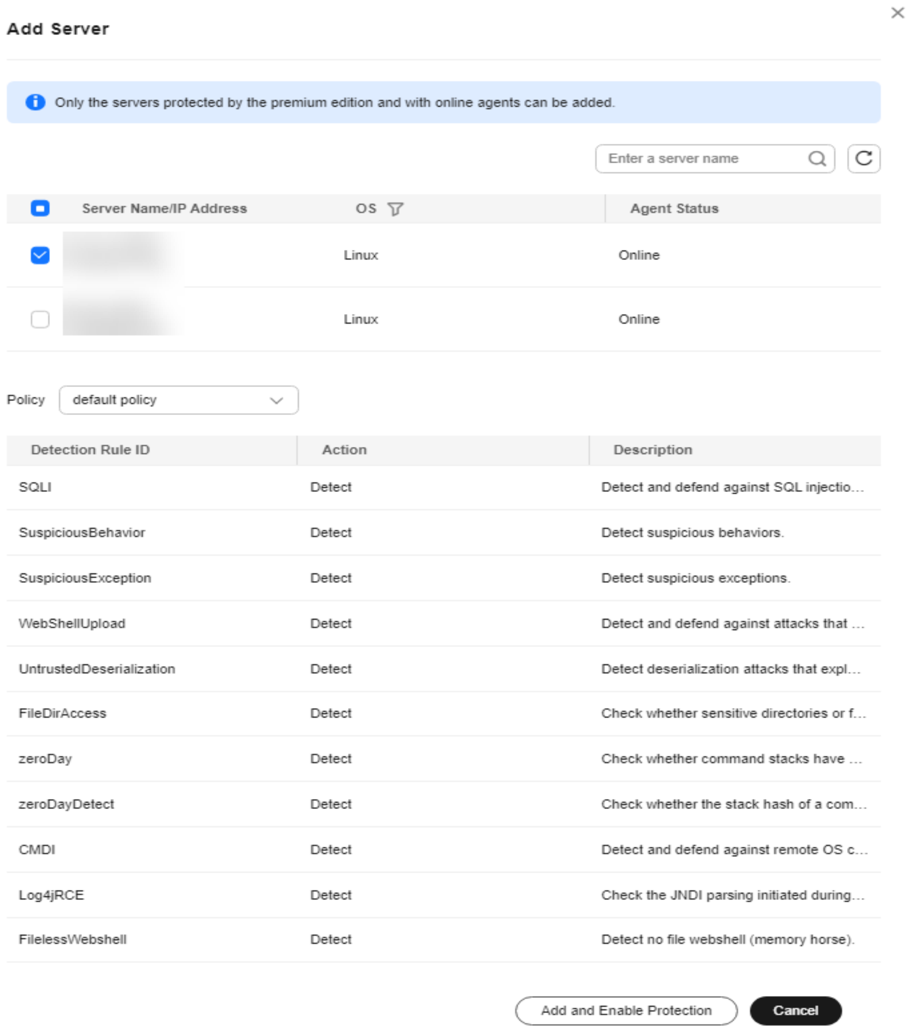
Server Name/ID	IP Address	OS	Server Group	Protection Policy	Protection Status	Microservice Pr...	RASP Protection	Detected Attacks	Operation
[redacted]	[redacted] Private)	Linux	editServerName-Dec...	default policy	● Protected	Configuration pending	Configuration pending	0	View Report Disable Protection

Step 4 Click **Add Server**. Select servers in the dialog box that is displayed.

NOTE

You can select a default security policy or create a security policy.

Figure 5-2 Selecting the target server and policy



Add Server

Only the servers protected by the premium edition and with online agents can be added.

Enter a server name

	Server Name/IP Address	OS	Agent Status
☑		Linux	Online
□		Linux	Online

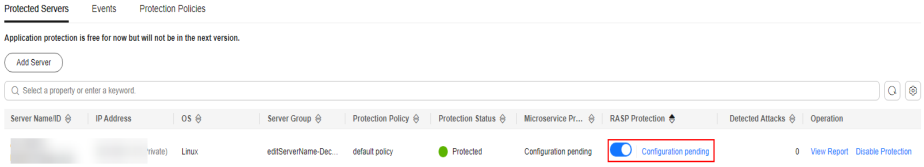
Policy: default policy

Detection Rule ID	Action	Description
SQLI	Detect	Detect and defend against SQL injectio...
SuspiciousBehavior	Detect	Detect suspicious behaviors.
SuspiciousException	Detect	Detect suspicious exceptions.
WebShellUpload	Detect	Detect and defend against attacks that ...
UntrustedDeserialization	Detect	Detect deserialization attacks that expl...
FileDirAccess	Detect	Check whether sensitive directories or f...
zeroDay	Detect	Check whether command stacks have ...
zeroDayDetect	Detect	Check whether the stack hash of a com...
CMDI	Detect	Detect and defend against remote OS c...
Log4jRCE	Detect	Check the JNDI parsing initiated during...
FilelessWebshell	Detect	Detect no file webshell (memory horse).

Step 5 Click **Add and Enable Protection**.

Step 6 On the **Protected Servers** tab, click the status in the **RASP Protection** column.

Figure 5-3 Viewing the progress of enabling protection



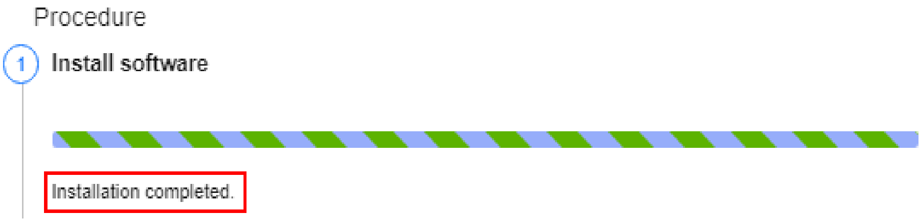
Application protection is free for now but will not be in the next version.

Select a property or enter a keyword.

Server Name/ID	IP Address	OS	Server Group	Protection Policy	Protection Status	Microservice Pr...	RASP Protection	Detected Attacks	Operation
	rivate)	Linux	editServerName-Dec...	default policy	● Protected	Configuration pending	Configuration pending	0	View Report Disable Protection

Step 7 Check the RASP software installation progress. Wait until the message "Installation completed." is displayed.

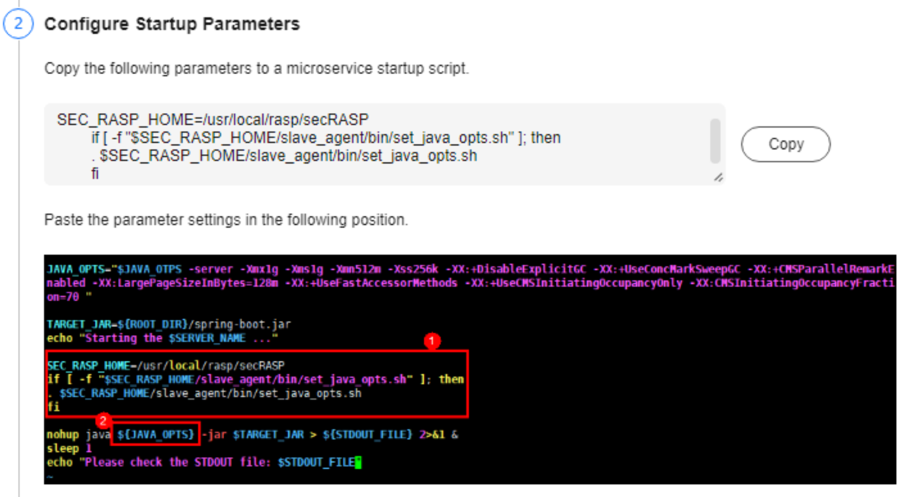
Figure 5-4 Installation completed



Installation completed.

Step 8 Log in to the server, go to the Spring Boot startup path, and copy the parameters from the **Configure Startup Parameters** step to the command box.

Figure 5-5 Configuring startup parameters



Copy the following parameters to a microservice startup script.

```
SEC_RASP_HOME=/usr/local/rasp/secRASP
      if [ -f "$SEC_RASP_HOME/slave_agent/bin/set_java_opts.sh" ]; then
      . $SEC_RASP_HOME/slave_agent/bin/set_java_opts.sh
      fi
```

Paste the parameter settings in the following position.

```
JAVA_OPTS="$JAVA_OTPS -server -Xmx1g -Xms1g -Xmn512m -Xss256k -XX:+DisableExplicitGC -XX:+UseConcMarkSweepGC -XX:+CMSParallelRemarkE
nabled -XX:LargePageSizeInBytes=128m -XX:+UseFastAccessorMethods -XX:+UseCMSInitiatingOccupancyOnly -XX:CMSInitiatingOccupancyFracti
on=70 "

TARGET_JAR=${ROOT_DIR}/spring-boot.jar
echo "Starting the $SERVER_NAME ..."

SEC_RASP_HOME=/usr/local/rasp/secRASP
if [ -f "$SEC_RASP_HOME/slave_agent/bin/set_java_opts.sh" ]; then
. $SEC_RASP_HOME/slave_agent/bin/set_java_opts.sh
fi

nohup java ${JAVA_OPTS} -jar $TARGET_JAR > ${STDOUT_FILE} 2>&1 &
sleep 1
echo "Please check the STDOUT file: $STDOUT_FILE"
~
```

Step 9 Restart the microservice to apply the protection settings.

Step 10 On the **Protected Servers** tab, check the protection status in the **Microservice Protection** column. If the status is **Active**, the protection has been enabled.

----End

5.1.2 Viewing Application Protection

After application protection is enabled, you can view the application protection status and events on the application protection page.

Prerequisites

Application protection has been enabled. For details, see **Enabling Application Protection**.

Constraints

- Currently, only Linux servers are supported.
- So far, only Java applications can be protected.
- The premium, WTP, and container editions support operations related to application protection.

Viewing Protection Settings

Step 1 Log in to the management console.

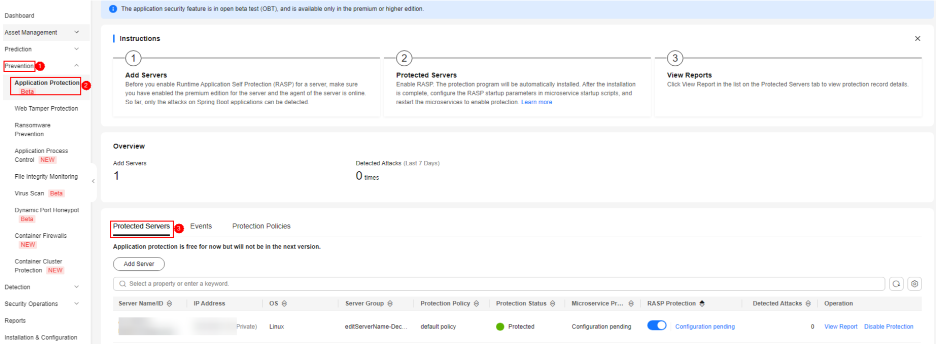
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Prevention** > **Application Protection**. Click the **Protected Servers** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-6 Viewing protection settings



The application security feature is in open beta test (OBT), and is available only in the premium or higher edition.

Instructions

1 Add Servers
Before you enable Runtime Application Self Protection (RASP) for a server, make sure you have enabled the premium edition for the server and the agent of the server is online. So far, only the attacks on Spring Boot applications can be detected.

2 Protected Servers
Enable RASP. The protection program will be automatically installed. After the installation is complete, configure the RASP startup parameters in microservice startup scripts, and restart the microservices to enable protection. Learn more

3 View Reports
Click View Report in the list on the Protected Servers tab to view protection record details.

Overview

Add Servers
1

Detected Attacks (Last 7 Days)
0 times

Application protection is free for now but will not be in the next version.

Select a property or enter a keyword.

Server Name/ID	IP Address	OS	Server Group	Protection Policy	Protection Status	Microservice Pr...	RASP Protection	Detected Attacks	Operation
[redacted]	[redacted] Private)	Linux	editServerName-Dec...	default policy	● Protected	Configuration pending	Configuration pending	0	View Report Disable Protection

Step 4 Click the **Protection Servers** tab and check the server list. The server parameters are as follows.

Table 5-1 Parameter description

Parameter	Description
Server Name/ID	Server name and ID
IP Address	Private IP address and EIP of the server
OS	Server OS
Server Group	Group that the server belongs to
Policy	Detection policies bound to the target server.
Protection Status	Agent status of a server. ● Protected: The agent is online. ● Unprotected: The agent is offline.

Parameter	Description
Microservice Protection	Microservice protection status. Its value can be: ● Effective: The microservice protection is enabled successfully. ● Installing: The microservice RASP protection software is being installed and protection is disabled. ● Installed but not configured: The microservice RASP protection software is successfully installed, but microservice startup parameters are not configured and protection is disabled. ● Installation failed: The microservice RASP protection software fails to be installed.
RASP Protection.	RASP protection status. Its value can be: If the following information is displayed, protection is not enabled. Check whether there are operations that are not handled by referring to **Enabling Application Protection**.
Detected Attacks	Number of attacks detected by RASP.

----End

Viewing Events

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Prevention** > **Application Protection** and click the **Events** tab. For details about the parameters, see **Table 5-2**.

To view the events of a server, click **View Report** in the **Operation** column of the target server.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Table 5-2 Event parameters

Parameter	Description
Severity	Alarm severity. You can search for servers by alarm severities. ● **Critical** ● **High** ● **Medium** ● **Low**

Parameter	Description
Server Name	Server that triggers an alarm
Alarm Name	Alarm name
Alarm Time	Time when an alarm is reported
Attack Source IP Address	IP address of the server that triggers the alarm
Attack Source URL	URL of the server that triggers the alarm

Step 3 You can click an alarm name to view the attack information (such as the request information and attack source IP address) and extended information (such as detection rule ID and description), and troubleshoot the problem accordingly.

----End

5.1.3 Managing Application Protection Policies

You can add, edit, and delete application protection policies, and select and configure detection rules for the policies.

Constraints

- Currently, only Linux servers are supported.
- So far, only Java applications can be protected.
- The premium, WTP, and container editions support operations related to application protection.

Adding 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** > **HSS**.

Step 3 Choose **Prevention** > **Application Protection** and click **Protection Policies**. For details about the parameters, see **Table 5-3**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

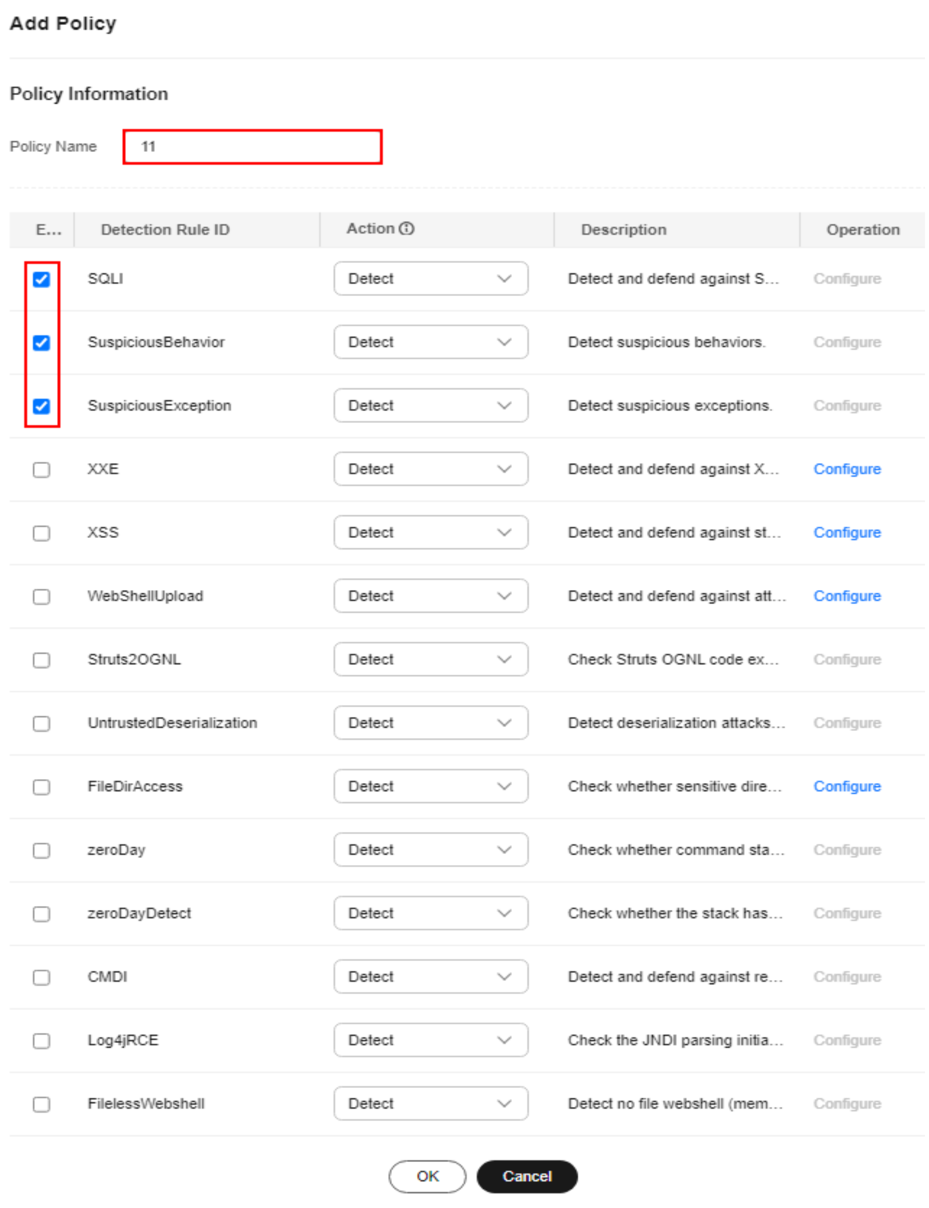
Table 5-3 Protection policy parameters

Parameter	Description
Policy Name	Protection policy name
Detection Rule	Detection rules supported by a policy.

Parameter	Description
Associated Servers	Number of servers bound to a policy.

Step 4 Click **Add Policy**. In the dialog box that is displayed, enter the policy name, select the rules to be detected, and configure details about some detection rules. For details about the parameters, see **Table 5-4**.

Figure 5-7 Adding a protection policy



Add Policy

Policy Information

Policy Name: 11

E...	Detection Rule ID	Action	Description	Operation
☑	SQLI	Detect	Detect and defend against S...	Configure
☑	SuspiciousBehavior	Detect	Detect suspicious behaviors.	Configure
☑	SuspiciousException	Detect	Detect suspicious exceptions.	Configure
□	XXE	Detect	Detect and defend against X...	Configure
□	XSS	Detect	Detect and defend against st...	Configure
□	WebShellUpload	Detect	Detect and defend against att...	Configure
□	Struts2OGNL	Detect	Check Struts OGNL code ex...	Configure
□	UntrustedDeserialization	Detect	Detect deserialization attacks...	Configure
□	FileDirAccess	Detect	Check whether sensitive dire...	Configure
□	zeroDay	Detect	Check whether command sta...	Configure
□	zeroDayDetect	Detect	Check whether the stack has...	Configure
□	CMDI	Detect	Detect and defend against re...	Configure
□	Log4jRCE	Detect	Check the JNDI parsing initia...	Configure
□	FilelessWebshell	Detect	Detect no file webshell (mem...	Configure

Table 5-4 Application protection policy parameters

Parameter	Description
Policy Name	User-defined policy name

Parameter	Description
Enabled	Whether to enable a detection rule for the current policy. You can select detection rules to enable them as required.
Detection Rule ID	ID of a detection rule
Action	Protection action of a detection rule. ● **Detect**: Detects objects based on the target rule and reports alarms for detected risk events. ● **Detect and block**: Detects objects based on the target rule, reports alarms for detected risk events, and directly blocks or intercepts detected risk items. **NOTICE** Blocking or interception may interrupt services. Exercise caution when enabling this function
Description	Description about the detected object and behavior of the target protection policy.

Step 5 Click **Configure** in the **Operation** column of a detection rule to modify the rule content. **Table 5-5** describes the supported detection rules.

Table 5-5 Detection rules that can be configured only

Rule	Description	Example
XXE	User-defined XXE blacklist protocol	.xml;.dtd;
XSS	User-defined XSS shielding rules	xml;doctype;xmlns;import;entity
WebShellUpload	User-defined suffix of files in the blacklist.	.jspx;.jsp;.jar;.phtml;.asp;.php;.ascx;.ashx;.cer
FileDirAccess	User-defined path of files in the blacklist.	/etc/passwd;/etc/shadow;/etc/gshadow;

Step 6 Confirm the configured policy and selected detection rules, and click **OK**. You can check whether the rule is added on the **Protection Policy** tab page.

----End

Editing a Protection Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Prevention** > **Application Protection** and click **Protection Policies**. For details about the parameters, see **Table 5-6**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Table 5-6 Protection policy parameters

Parameter	Description
Policy Name	Protection policy name
Detection Rule	Detection rules supported by a policy.
Associated Servers	Number of servers bound to a policy.

Step 3 Click **Edit** in the **Operation** column of a policy to configure the policy name, supported detection rules, and rule content.

Table 5-7 Application protection policy parameters

Parameter	Description
Policy Name	User-defined policy name
Enabled	Whether to enable a detection rule for the current policy. You can select detection rules to enable them as required.
Detection Rule ID	ID of a detection rule
Action	Protection action of a detection rule. ● **Detect**: Detects objects based on the target rule and reports alarms for detected risk events. ● **Detect and block**: Detects objects based on the target rule, reports alarms for detected risk events, and directly blocks or intercepts detected risk items. NOTICE Blocking or interception may interrupt services. Exercise caution when enabling this function
Description	Description about the detected object and behavior of the target protection policy.

Step 4 Confirm the configured rule and selected detection items and click **OK**. You can check whether the target policy is modified on the **Protection Policy** tab page.

----End

Deleting a Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Prevention** > **Application Protection** and click **Protection Policies**. For details about the parameters, see **Table 5-8**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Table 5-8 Protection policy parameters

Parameter	Description
Policy Name	Protection policy name
Detection Rule	Detection rules supported by a policy.
Associated Servers	Number of servers bound to a policy.

Step 3 Click **Delete** in the **Operation** column of the target policy. In the dialog box that is displayed, confirm the policy information and click **OK**.

NOTICE

If the policy to be deleted is associated with a server, bind the server to another protection policy first. Otherwise, the **Delete** button of the target policy is hidden.

----End

5.1.4 Disabling Application Protection

This section describes how to disable application protection.

Procedure

Step 1 Log in to the management console.

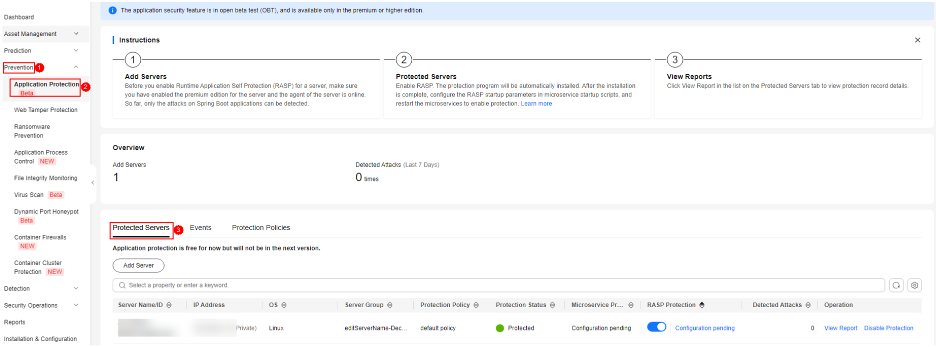
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Prevention** > **Application Protection**. Click the **Protected Servers** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-8 Viewing protection settings



Dashboard
Asset Management
Prediction
Prevention
1
Application Protection Beta
2
Web Tamper Protection
Ransomware Prevention
Application Process Control NEW
File Integrity Monitoring
Virus Scan Beta
Dynamic Port Honeypot Beta
Container Firewalls NEW
Container Cluster Protection NEW
Detection
Security Operations
Reports
Installation & Configuration
3

The application security feature is in open beta test (OBT), and is available only in the premium or higher edition.

Instructions

1 **Add Servers**
Before you enable Runtime Application Self Protection (RASP) for a server, make sure you have enabled the premium edition for the server and the agent of the server is online. So far, only the attacks on Spring Boot applications can be detected.

2 **Protected Servers**
Enable RASP. The protection program will be automatically installed. After the installation is complete, configure the RASP startup parameters in microservice startup scripts, and restart the microservices to enable protection. Learn more

3 **View Reports**
Click View Report in the list on the Protected Servers tab to view protection record details.

Overview

Add Servers: 1

Detected Attacks (Last 7 Days): 0 times

Protected Servers | Events | Protection Policies

Application protection is free for now but will not be in the next version.

Add Server

Select a property or enter a keyword.

Server Name/ID	IP Address	OS	Server Group	Protection Policy	Protection Status	Microservice Pr...	RASP Protection	Detected Attacks	Operation
[redacted]	[redacted]Private)	Linux	editServerName-Dec...	default policy	● Protected	Configuration pending	Configuration pending	0	View Report Disable Protection

Step 4 Toggle off the switch in the **RASP Protection** column or click **Disable Protection** in the **Operation** column.

Step 5 In the dialog box that is displayed, confirm the server information and click **OK**.

NOTE

After RASP is disabled for a server, the server will be removed from the **Protected Servers** tab. For details about how to enable protection, see **Enabling Application Protection**.

----End

5.2 WTP

5.2.1 WTP Overview

Web Tamper Protection (WTP) can detect and prevent tampering of files in specified directories, including web pages, documents, and images, and quickly restore them using valid backup files.

Constraints

Ensure that the WTP edition has been enabled for the server. For details about how to purchase HSS and enable the WTP edition, see **Purchasing HSS Quota** and **Enabling Web Tamper Protection**.

How WTP Prevents Web Page Tampering

WTP supports static and dynamic web page protection. **How WTP works** shows the protection mechanism.

Table 5-9 How WTP works

Protection 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 the file and backup directory on the local server become invalid, you can manually obtain the backup file from the remote backup server to restore the tampered websites.

Protection Type	Mechanism
Dynamic web page protection	Provides runtime application self-protection (RASP) for Tomcat applications in the following ways: 1. Malicious behavior filtering based on RASP The Huawei-unique runtime application self-protection (RASP) detects application program behaviors, preventing attackers from tampering with web pages through application programs. 2. Network disk file access control WTP implements fine-grained management to control permissions for adding, modifying, and querying file content in network disks, preventing tampering without affecting website content release.

Process of Using WTP

Figure 5-9 Usage process

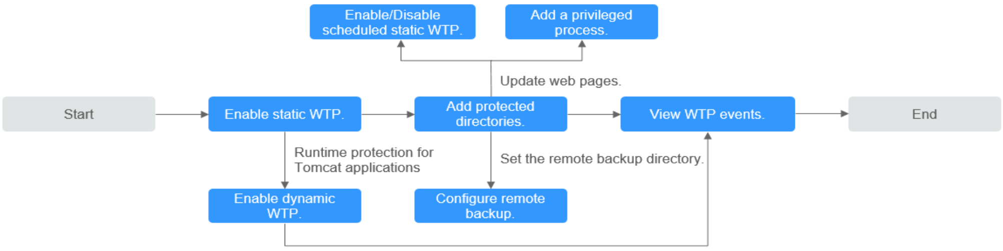

Enable/Disable scheduled static WTP.
Add a privileged process.
Update web pages.
Start
Enable static WTP.
Add protected directories.
View WTP events.
End
Runtime protection for Tomcat applications
Set the remote backup directory.
Enable dynamic WTP.
Configure remote backup.

Table 5-10 Process of using WTP

Operation	Description
Enabling Static Web Tamper Protection	After the WTP edition is enabled, static WTP and other protection functions are enabled automatically. For details about the functions supported by the WTP edition, see **Editions and Features**.
Adding a Protected Directory	Static WTP protects specified directories. You need to configure static WTP directories.
Configuring Remote Backup	By default, HSS backs up files in the protected directories to the local backup paths you specified when adding protected directories. To prevent the local backup from being damaged by attackers, you can configure remote backup to protect web page backup data.

Operation	Description
Adding a Privileged Process	After static WTP is enabled, the content in the protected directory is read-only and cannot be modified. To modify a protected file, you can add a privileged process.
Enabling/ Disabling Scheduled Static WTP	Not all OS kernel versions support privileged processes and each server can add up to 10 privileged processes. For OSs that do not support privileged processes, you can set periodic static WTP and update websites when WTP is automatically disabled.
Enabling Dynamic WTP	HSS provides runtime application self-protection (RASP) for Tomcat applications. You can enable dynamic WTP for Tomcat applications as required.
Viewing WTP Events	Tamper events that occur during static web tamper protection are recorded and displayed in the event list.

5.2.2 Adding a Protected Directory

WTP monitors website directories in real time, backs up files, and restores tampered files using the backup, protecting websites from Trojans, illegal links, and tampering.

Prerequisites

You have enabled the WTP edition.

Constraints and Limitations

- Only the servers that are protected by the HSS WTP edition support the operations described in this section.
- The constraints on protected directories are as follows:
  - For Linux,
    - A server can have up to 50 protected directories.
    - The complete path of a protected directory cannot exceed 256 characters.
    - The folder levels of a protected directory cannot exceed 100.
    - The total folders in protected directories cannot exceed 900,000.
  - For Windows,
    - A server can have up to 50 protected directories.
    - The complete path of a protected directory cannot exceed 256 characters.
- The constraints on local backup paths are as follows:

- – Local backup is supported only in Linux.
- – The local backup path must be valid, or web tamper protection will not take effect.
- – The local backup path cannot overlap with the added protected directory.
- – The available capacity of the disk where the local backup path is located is greater than the size of all protected directories.

Adding a Protected Directory

Step 1 Log in to the management console.

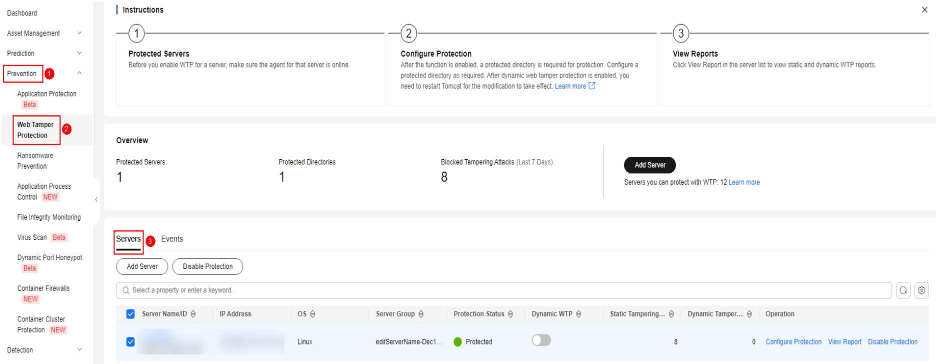
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Prevention** > **Web Tamper Protection**, click **Configure Protection**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-10 Entering the page for protected directory settings



1 Protected Servers
Before you enable WTP for a server, make sure the agent for that server is online.

2 Configure Protection
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

3 View Reports
Click View Report in the server list to view static and dynamic WTP reports.

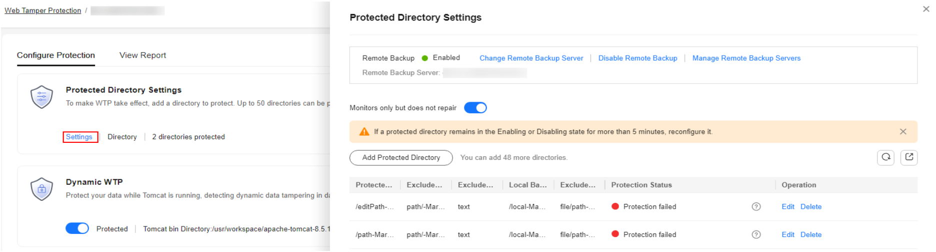
Protected Servers	Protected Directories	Blocked Tampering Attacks (Last 7 Days)
1	1	8

Servers you can protect with WTP: 12 Learn more

☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑			Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 4 Click **Settings** under **Protected Directory Settings**.

Figure 5-11 Page for setting a protected directory



Protected Directory Settings
To make WTP take effect, add a directory to protect. Up to 50 directories can be p

Settings | Directory | 2 directories protected

Dynamic WTP
Protect your data while Tomcat is running, detecting dynamic data tampering in da

Protected | Tomcat bin Directory:/usr/workspace/apache-tomcat-8.5.1

Remote Backup ● Enabled
Remote Backup Server:

Monitors only but does not repair

If a protected directory remains in the Enabling or Disabling state for more than 5 minutes, reconfigure it.

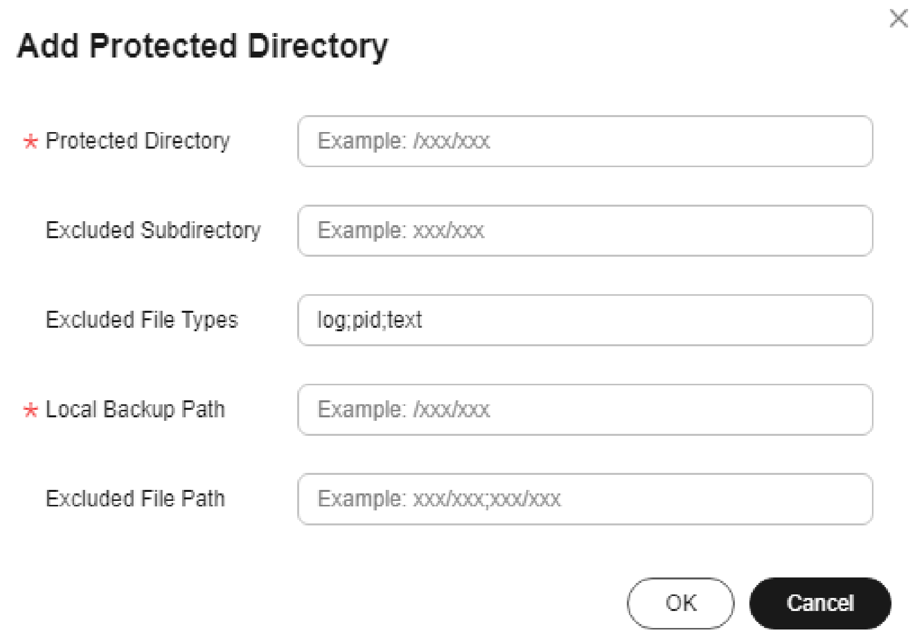
You can add 48 more directories.

Protecte...	Exclude...	Exclude...	Local Ba...	Exclude...	Protection Status		Operation
/editPath-...	path/-Mar...	text	/local-Ma...	file/path-...	● Protection failed	ⓘ	Edit Delete
/path-Mar...	path/-Mar...	text	/local-Ma...	file/path-...	● Protection failed	ⓘ	Edit Delete

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 5-11**.

Figure 5-12 Adding a protected directory



Add Protected Directory

* Protected Directory: Example: /xxx/xxx

Excluded Subdirectory: Example: xxx/xxx

Excluded File Types: log;pid;text

* Local Backup Path: Example: /xxx/xxx

Excluded File Path: Example: xxx/xxx;xxx/xxx

Table 5-11 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.
Excluded Subdirectory	– Subdirectories that do not need to be protected in the protected directory, such as temporary file directories. – Separate subdirectories with semicolons (;). A maximum of 10 subdirectories can be added.	The subdirectory is a relative directory in the protected directory.

Paramete r	Description	Restriction
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	– Only Linux is supported. – 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.

Parameter	Description	Restriction
Excluded File Path	– Paths that do not need to be protected in the protected directory. – Separate multiple paths with semicolons (;). A maximum of 50 paths can be added. The maximum length of a path is 256 characters. – A single path cannot start with a space or end with a slash (/).	The excluded file path is the relative file path of the 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.

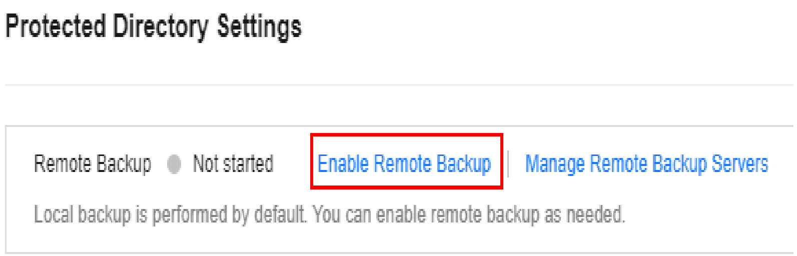
Step 6 Enable remote backup.

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 **Configuring Remote Backup**.

1. On the **Protected Directory Settings** page, click **Enable Remote Backup**.

   Figure 5-13 Enabling remote backup



Protected Directory Settings

Remote Backup ● Not started

Local backup is performed by default. You can enable remote backup as needed.

2. Select a backup server from the drop-down list box.
3. Click **OK**.

----End

Related Operations

- Export a protected directory: If you have configured a large number of protected directories, you can click ⧉ on the protected directory configuration page to export the configurations of all protected directories to your local PC.

- Suspend protection: You can suspend WTP for a directory if needed. It is recommended 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.

5.2.3 Configuring 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.

If the file and backup directory on the local server become invalid, you can manually obtain the backup file from the remote backup server to restore the tampered websites.

Constraints

Only the servers that are protected by the HSS WTP edition support the operations described in this section.

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.

Adding a Remote Backup Server

Step 1 Log in to the management console.

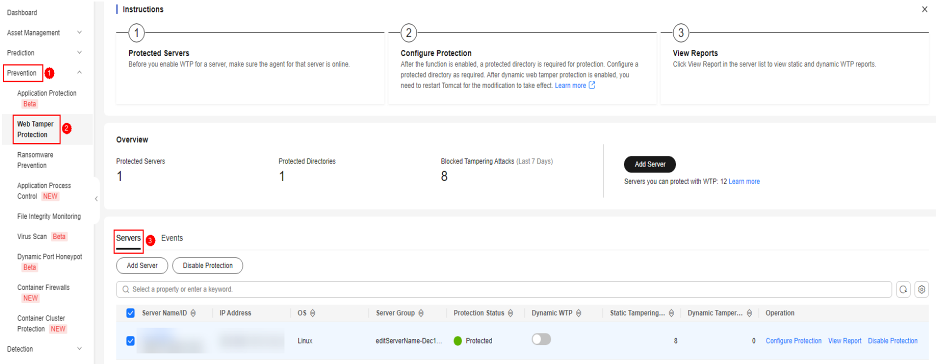
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Prevention** > **Web Tamper Protection**, click **Configure Protection**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-14 Entering the page for protected directory settings



Protected Servers
Before you enable WTP for a server, make sure the agent for that server is online.

Configure Protection
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

View Reports
Click View Report in the server list to view static and dynamic WTP reports.

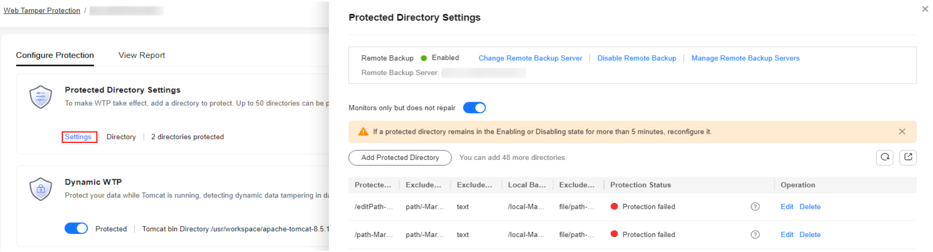
Protected Servers: 1
Protected Directories: 1
Blocked Tampering Attacks (Last 7 Days): 8

Servers you can protect with WTP: 12 Learn more

☑ Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑ [redacted]	[redacted]	Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 4 Click **Settings** under **Protected Directory Settings**.

Figure 5-15 Page for setting a protected directory



To make WTP take effect, add a directory to protect. Up to 50 directories can be p

Settings | Directory | 2 directories protected

Protect your data while Tomcat is running, detecting dynamic data tampering in d

Protected | Tomcat bin Directory:/usr/workspace/apache-tomcat-8.5.1

Remote Backup ● Enabled
Remote Backup Server: [redacted]

Monitors only but does not repair: on

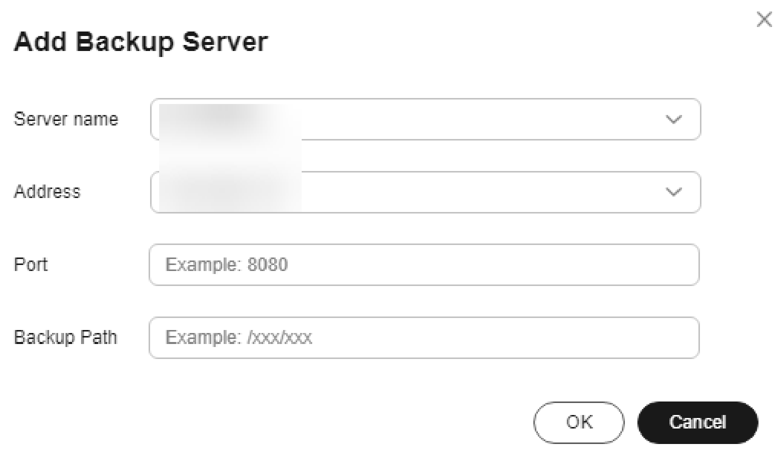
If a protected directory remains in the Enabling or Disabling state for more than 5 minutes, reconfigure it.

You can add 48 more directories.

Protecte...	Exclude...	Exclude...	Local Ba...	Exclude...	Protection Status	Operation
/editPath-...	path/-Mar...	text	/local-Ma...	file/path-...	● Protection failed	Edit Delete
/path-Mar...	path/-Mar...	text	/local-Ma...	file/path-...	● Protection failed	Edit Delete

Step 5 Click **Manage Remote Backup**. In the dialog box that is displayed, click **Add Backup Server**. For details, see Table 5-12.

Figure 5-16 Configuring the backup server



Add Backup Server

Server name

Address

Port: Example: 8080

Backup Path: Example: /xxx/xxx

Table 5-12 Backup server parameters

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.
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 6 Click **OK**.

----End

Setting remote backup

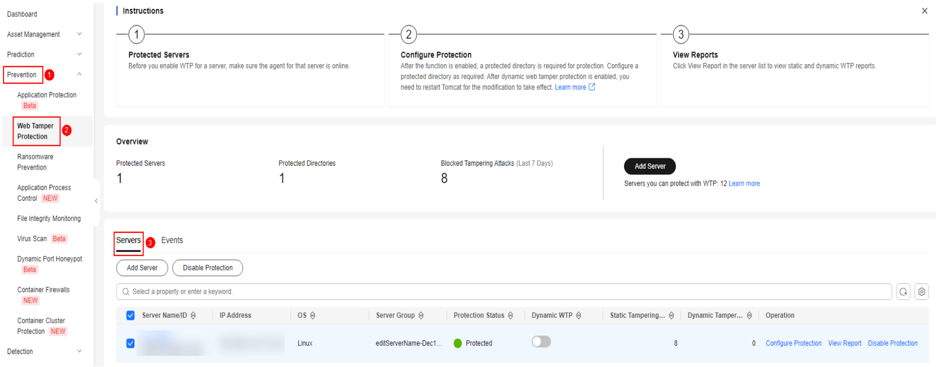
Step 1 Log in to the management console.

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

Step 3 Choose **Prevention** > **Web Tamper Protection**, click **Configure Protection**.

> NOTE
>
> If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-17 Entering the page for protected directory settings



1 **Protected Servers**
Before you enable WTP for a server, make sure the agent for that server is online.

2 **Configure Protection**
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

3 **View Reports**
Click View Report in the server list to view static and dynamic WTP reports.

Overview

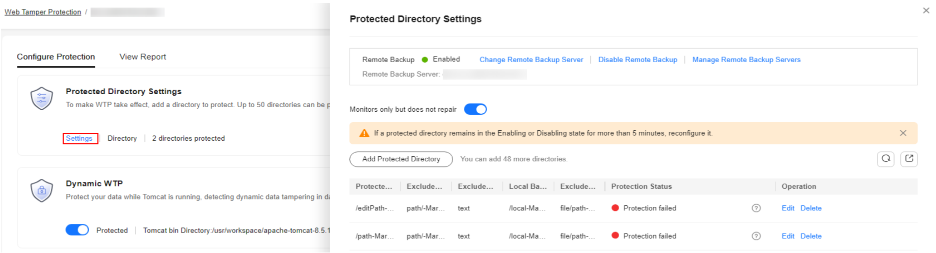
Protected Servers	Protected Directories	Blocked Tampering Attacks (Last 7 Days)
1	1	8

Add Server
Servers you can protect with WTP: 12 Learn more

☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑	[redacted]	[redacted]	Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 4 Click **Settings** under **Protected Directory Settings**.

Figure 5-18 Page for setting a protected directory



Protected Directory Settings
To make WTP take effect, add a directory to protect. Up to 50 directories can be p

Settings | Directory | 2 directories protected

Dynamic WTP
Protect your data while Tomcat is running, detecting dynamic data tampering in da

Protected | Tomcat bin Directory:/usr/workspace/apache-tomcat-8.5.1

Protected Directory Settings

Remote Backup ● Enabled Change Remote Backup Server | Disable Remote Backup | Manage Remote Backup Servers
Remote Backup Server: [redacted]

Monitors only but does not repair

If a protected directory remains in the Enabling or Disabling state for more than 5 minutes, reconfigure it.

You can add 48 more directories.

Protecte...	Exclude...	Exclude...	Local Ba...	Exclude...	Protection Status		Operation
/editPath-...	path/-Mar...	text	/local-Ma...	file/path-...	● Protection failed	ⓘ	Edit Delete
/path-Mar...	path/-Mar...	text	/local-Ma...	file/path-...	● Protection failed	ⓘ	Edit Delete

Step 5 Click **Enable Remote Backup** and select a remote backup server.

Step 6 Click **OK** to start remote backup.

----End

Changing a Remote Backup Server

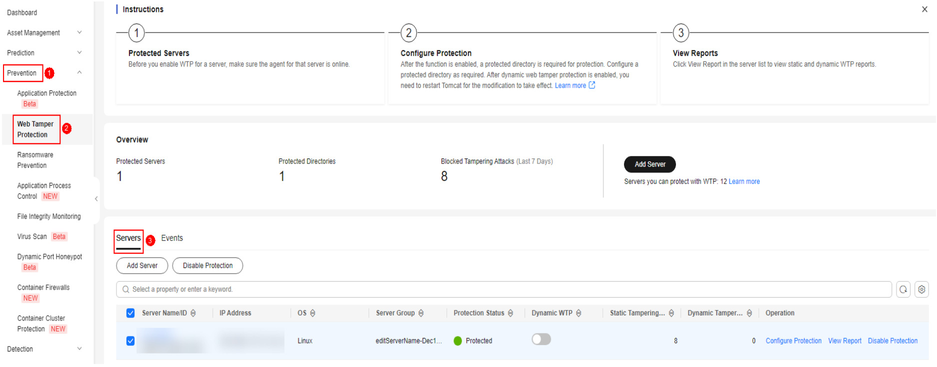
Step 1 Log in to the management console.

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

Step 3 Choose **Prevention** > **Web Tamper Protection**, click **Configure Protection**.

> NOTE
>
> If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-19 Entering the page for protected directory settings



Protected Servers
Before you enable WTP for a server, make sure the agent for that server is online.

Configure Protection
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

View Reports
Click View Report in the server list to view static and dynamic WTP reports.

Protected Servers	Protected Directories	Blocked Tampering Attacks (Last 7 Days)
1	1	8

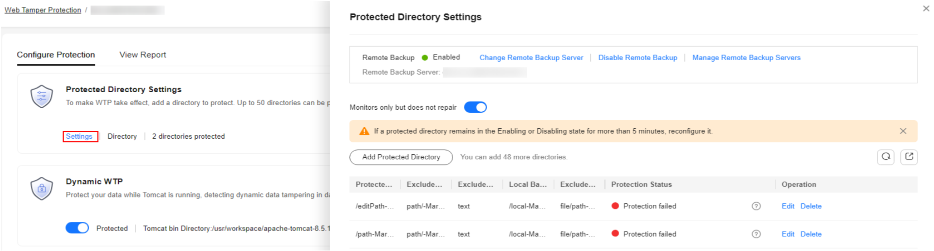
Servers you can protect with WTP: 12 Learn more

Select a property or enter a keyword.

☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑	[redacted]	[redacted]	Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 4 Click **Settings** under **Protected Directory Settings**.

Figure 5-20 Page for setting a protected directory



Protected Directory Settings
To make WTP take effect, add a directory to protect. Up to 50 directories can be p

Settings | Directory | 2 directories protected

Dynamic WTP
Protect your data while Tomcat is running, detecting dynamic data tampering in da

Protected | Tomcat bin Directory:/usr/workspace/apache-tomcat-8.5.1

Protected Directory Settings

Remote Backup ● Enabled Change Remote Backup Server | Disable Remote Backup | Manage Remote Backup Servers
Remote Backup Server: [redacted]

Monitors only but does not repair

If a protected directory remains in the Enabling or Disabling state for more than 5 minutes, reconfigure it.

You can add 48 more directories.

Protecte...	Exclude...	Exclude...	Local Ba...	Exclude...	Protection Status	Operation
/editPath-...	path/-Mar...	text	/local-Ma...	file/path-...	● Protection failed	Edit Delete
/path-Mar...	path/-Mar...	text	/local-Ma...	file/path-...	● Protection failed	Edit Delete

Step 5 Click **Change Remote Backup Server**. Select a remote backup server from the drop-down list.

NOTE

On the **Change Remote Backup Server** dialog box, the **Backup Server** you selected must have been **Enabled**.

Step 6 Click **OK**.

----End

Related Operations

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.

5.2.4 Adding a Privileged Process

If WTP is enabled, the content in the protected directories is read-only. To allow certain processes to modify files in the directories, 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.

Constraints

- Only the servers that are protected by the HSS WTP edition support the operations described in this section.
- For Linux OSs, only x86 OSs with kernel 4.18 support this function.
- The privileged process takes effect only for Agent 3.2.4 or later.
- A maximum of 10 privileged processes can be added to each server.

Prerequisites

The **Protection Status** of the server must be **Protected**. To view the status, choose **Prevention** > **Web Tamper Protection**. Click the **Servers** tab.

Adding a Privileged Process

Step 1 Log in to the management console.

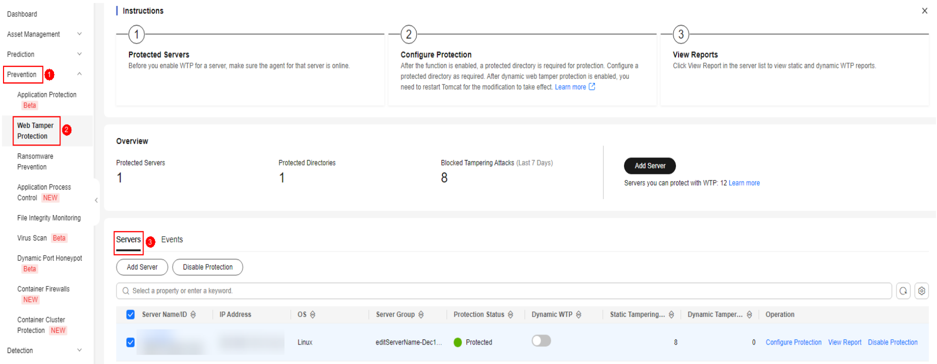
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Prevention** > **Web Tamper Protection**, click **Configure Protection**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-21 Entering the page for protected directory settings



Protected Servers
Before you enable WTP for a server, make sure the agent for that server is online.

Configure Protection
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

View Reports
Click View Report in the server list to view static and dynamic WTP reports.

Overview

Protected Servers	Protected Directories	Blocked Tampering Attacks (Last 7 Days)
1	1	8

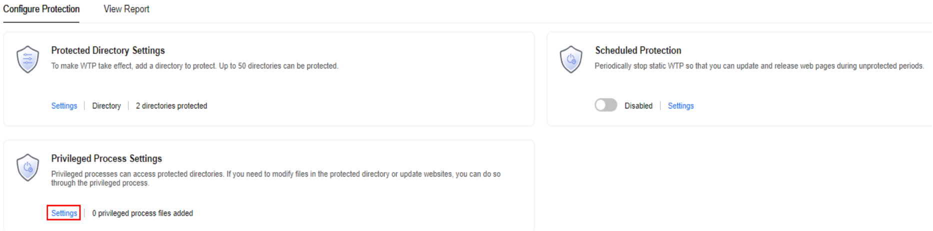
Servers you can protect with WTP: 12 Learn more

Select a property or enter a keyword.

☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑	[redacted]	[redacted]	Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 4 Click **Privileged Process Settings** and then **Settings**.

Figure 5-22 Setting a privileged process



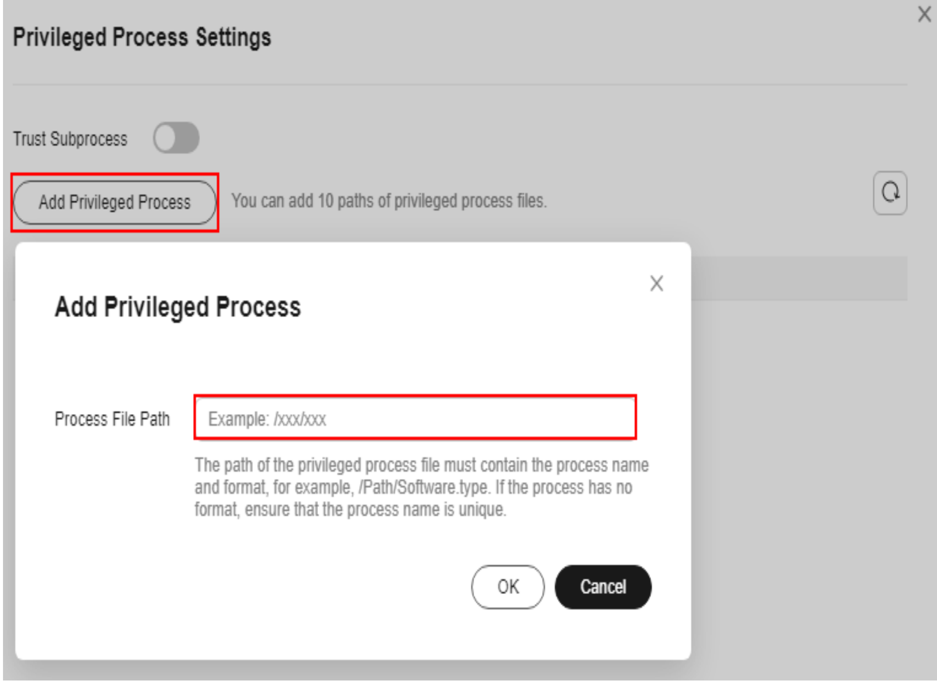
Protected Directory Settings
To make WTP take effect, add a directory to protect. Up to 50 directories can be protected.
Settings | Directory | 2 directories protected

Scheduled Protection
Periodically stop static WTP so that you can update and release web pages during unprotected periods.
Disabled | Settings

Privileged Process Settings
Privileged processes can access protected directories. If you need to modify files in the protected directory or update websites, you can do so through the privileged process.
Settings | 0 privileged process files added

Step 5 On the **Privileged Process Settings** page, click **Add Privileged Process**.

Figure 5-23 Adding a Privileged Process



Privileged Process Settings

Trust Subprocess

You can add 10 paths of privileged process files.

Add Privileged Process

Process File Path: Example: /xxx/xxx

The path of the privileged process file must contain the process name and format, for example, /Path/Software.type. If the process has no format, ensure that the process name is unique.

Step 6 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 7 Click **OK**.

Step 8 Enable **Trust Subprocess** to trust the subprocess in the path of the added privileged file.

NOTE

When this function is enabled, subprocesses at the five levels under all privileged process files are trusted.

----End

Related Operations

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 privileged processes should be deleted in a timely manner as they may be exploited by attackers.

5.2.5 Enabling/Disabling Scheduled Static WTP

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.

Constraints

Only the servers that are protected by the HSS WTP edition support the operations described in this section.

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 local time base.

Procedure

Step 1 Log in to the management console.

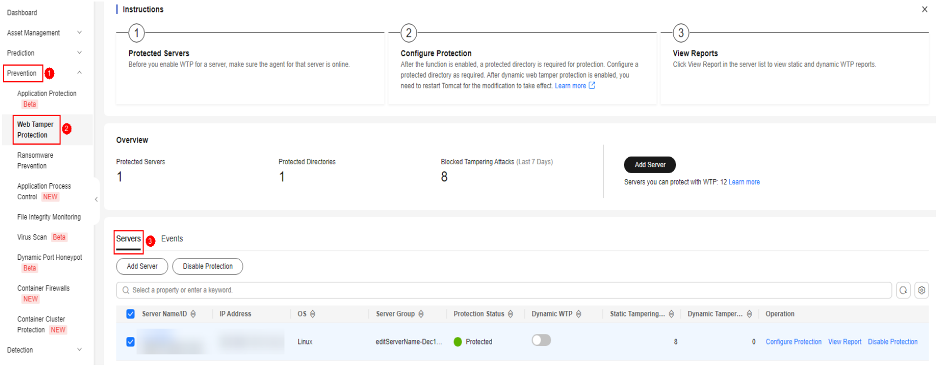
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Prevention** > **Web Tamper Protection**, click **Configure Protection**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-24 Entering the page for protected directory settings



Instructions

1 Protected Servers
Before you enable WTP for a server, make sure the agent for that server is online.

2 Configure Protection
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

3 View Reports
Click View Report in the server list to view static and dynamic WTP reports.

Overview

Protected Servers: 1
Protected Directories: 1
Blocked Tampering Attacks (Last 7 Days): 8

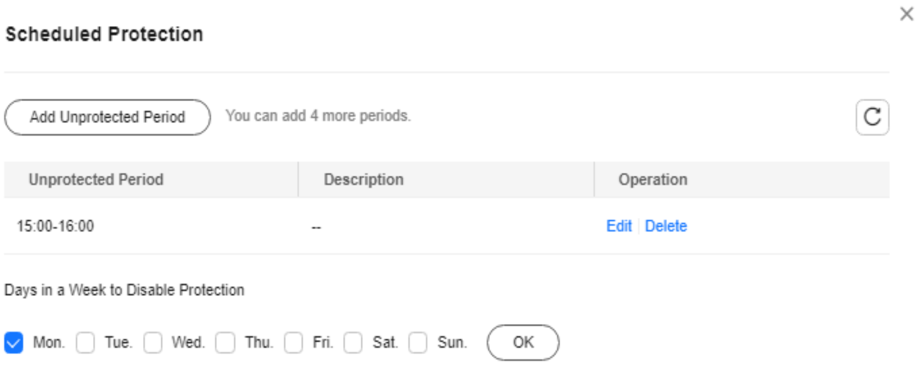
Servers you can protect with WTP: 12 Learn more

☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑			Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 4 On the **Configure Protection** tab, click **Settings** under **Scheduled Protection**.

Step 5 Set the unprotected period and days in a week to automatically disable protection.

Figure 5-25 Setting scheduled protection parameters



Scheduled Protection

Add Unprotected Period | You can add 4 more periods.

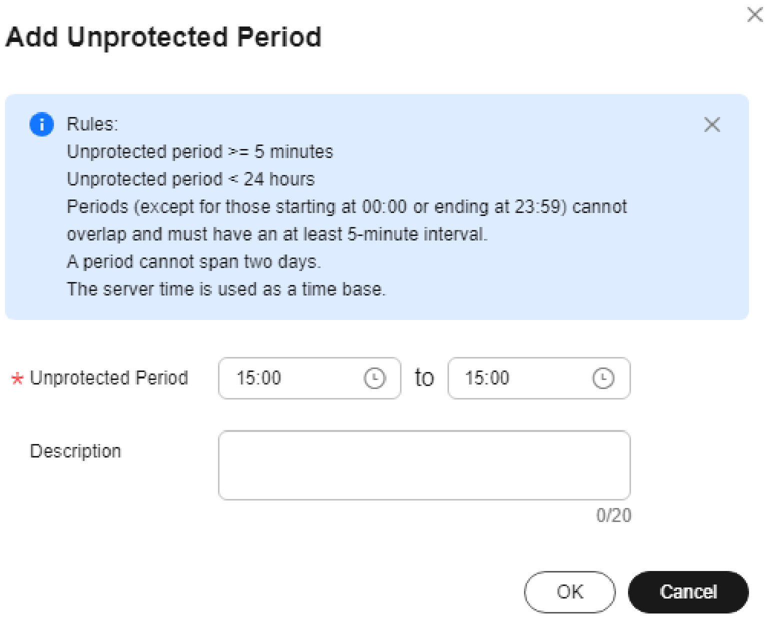
Unprotected Period	Description	Operation
15:00-16:00	--	Edit | Delete

Days in a Week to Disable Protection

☑ Mon. □ Tue. □ Wed. □ Thu. □ Fri. □ Sat. □ Sun. OK

1. Click **Add Unprotected Period**. Configure parameters in the dialog box that is displayed.

   Figure 5-26 Adding an unprotected period

   Add Unprotected Period

   Rules:
   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.

   * Unprotected Period: 15:00 to 15:00

   Description: 0/20

   OK Cancel

   NOTE

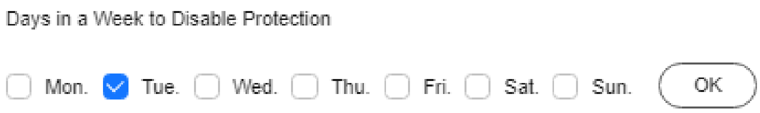
   Configuration constraints:

   - 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.

2. Click **OK**.
3. Select the days to disable protection.

   For example, if you select **Mon.**, **Thu.**, and **Sat.**, the server automatically disables the WTP function during the unprotected period on these days.

Figure 5-27 Selecting days to disable protection



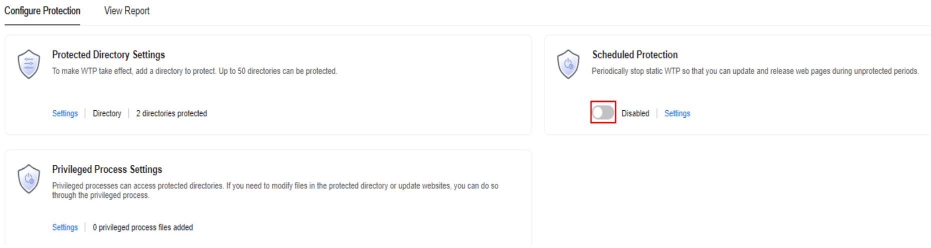
Days in a Week to Disable Protection

□ Mon. ☑ Tue. □ Wed. □ Thu. □ Fri. □ Sat. □ Sun. OK

4. Click **OK**.

Step 6 Return to the **Configure Protection** tab and toggle on to enable **Scheduled Protection**.

Figure 5-28 Enabling scheduled protection



Configure Protection View Report

Protected Directory Settings

To make WTP take effect, add a directory to protect. Up to 50 directories can be protected.

Settings | Directory | 2 directories protected

Scheduled Protection

Periodically stop static WTP so that you can update and release web pages during unprotected periods.

Disabled | Settings

Privileged Process Settings

Privileged processes can access protected directories. If you need to modify files in the protected directory or update websites, you can do so through the privileged process.

Settings | 0 privileged process files added

----End

5.2.6 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.

Constraints and Limitations

- Only the servers that are protected by the HSS WTP edition support the operations described in this section.
- Dynamic WTP can be provided only for Tomcat of JDK 8.

Prerequisites

You are using a server running the Linux OS.

Procedure

Step 1 Log in to the management console.

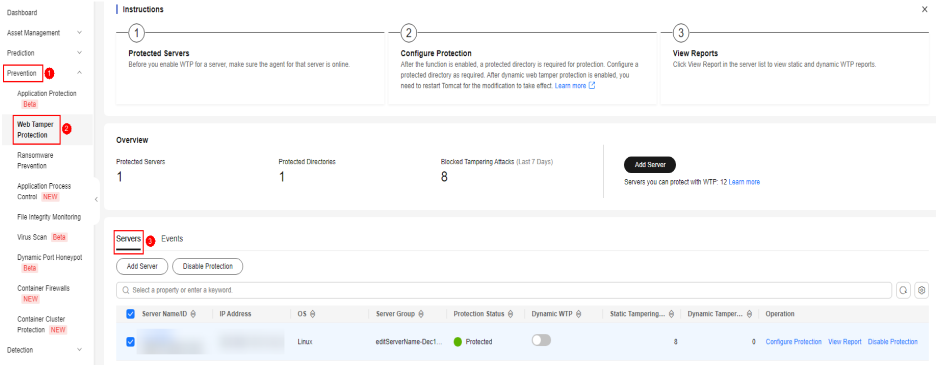
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Prevention** > **Web Tamper Protection**, click **Configure Protection**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 5-29 Entering the page for protected directory settings



Protected Servers
Before you enable WTP for a server, make sure the agent for that server is online.

Configure Protection
After the function is enabled, a protected directory is required for protection. Configure a protected directory as required. After dynamic web tamper protection is enabled, you need to restart Tomcat for the modification to take effect. Learn more

View Reports
Click View Report in the server list to view static and dynamic WTP reports.

Overview

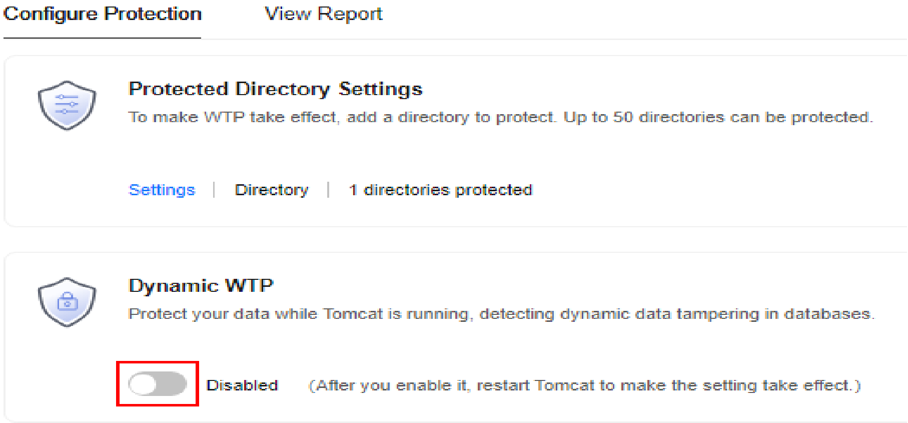
Protected Servers	Protected Directories	Blocked Tampering Attacks (Last 7 Days)
1	1	8

Servers you can protect with WTP: 12 Learn more

☑	Server Name/ID	IP Address	OS	Server Group	Protection Status	Dynamic WTP	Static Tampering...	Dynamic Tamper...	Operation
☑	[redacted]	[redacted]	Linux	editServerName-Dec1...	● Protected	○	8	0	Configure Protection View Report Disable Protection

Step 4 On the **Configure Protection** tab, toggle on ○ to enable **Dynamic WTP**.

Figure 5-30 Enabling Dynamic WTP



Protected Directory Settings
To make WTP take effect, add a directory to protect. Up to 50 directories can be protected.

1 directories protected

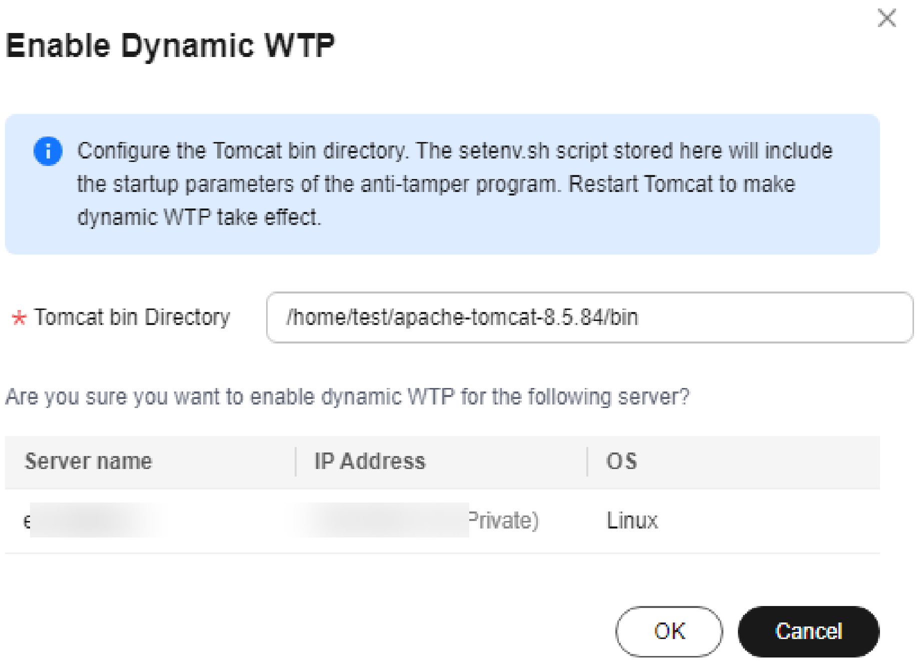
Dynamic WTP
Protect your data while Tomcat is running, detecting dynamic data tampering in databases.

○ Disabled (After you enable it, restart Tomcat to make the setting take effect.)

Step 5 In the displayed dialog box, modify the **Tomcat bin Directory**.

To enable dynamic WTP, you need to modify the Tomcat bin directory first. The system presets the **setenv.sh** script in the bin directory for setting anti-tamper program startup parameters. After enabling dynamic WTP, restart Tomcat to make this setting take effect.

Figure 5-31 Configuring a Tomcat directory



Enable Dynamic WTP

Configure the Tomcat bin directory. The setenv.sh script stored here will include the startup parameters of the anti-tamper program. Restart Tomcat to make dynamic WTP take effect.

* Tomcat bin Directory: /home/test/apache-tomcat-8.5.84/bin

Are you sure you want to enable dynamic WTP for the following server?

Server name	IP Address	OS
[redacted]	[redacted]Private)	Linux

Step 6 Click **OK** to enable dynamic WTP.

----End

5.2.7 Viewing WTP Events

Once static WTP is enabled, the HSS service will comprehensively check protected directories you specified. You can check records about detected tampering of host protection files.

Constraints

Only the servers that are protected by the HSS WTP edition support the operations described in this section.

Prerequisites

- **Agent Status** of the server is **Online**, and its **WTP Status** is **Enabled**.
- WTP is enabled.

Procedure

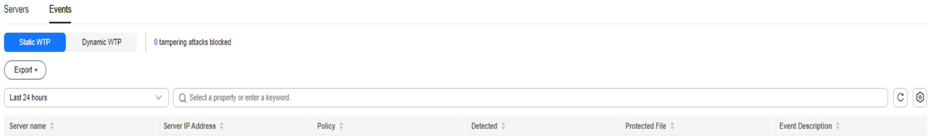
Step 1 Log in to the management console.

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

Step 3 Choose **Prevention** > **Web Tamper Protection** and click **Events** to view the tampering records of protected files on servers.

To view the events of a server, click **View Report** in the **Operation** column of the target server.

Figure 5-32 Events



0 tampering attacks blocked

Server name	Server IP Address	Policy	Detected	Protected File	Event Description

----End

5.3 Ransomware Prevention

5.3.1 Purchasing a Backup Vault

To enhance defense and reduce service loss caused by ransomware attacks, you are advised to periodically back up data on servers. Before enabling backup, purchase a vault to be used for backup storage.

You can purchase a backup vault on the HSS console by referring to this section, or on the CBR console by referring to**Creating a cloud server backup Backup**.

Purchasing a Backup Vault

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** > **HSS**.

Step 3 Choose **Prevention** > **Ransomware Prevention**.

Step 4 Click the **Protected Servers** tab.

Step 5 Toggle on ransomware backup. In the dialog box that is displayed, click **Next**.

Step 6 In the displayed dialog box, set the vault parameters.

Table 5-13 Parameters for purchasing backup capacity

Parameter	Description
Billing Mode	Select **Yearly/Monthly** or **On-demand** as required. ● **Yearly/Monthly**: You are billed based on the purchase period specified in the order. ● **On-demand**: You pay for the duration you use the resources. Prices are calculated by hour, and no minimum fee is required.
Region	Region of the backup vault you want to purchase
Capacity	Select the size of the backup vault as required.
Required Duration	Select the required duration if you selected **Yearly/Monthly** for **Billing Mode**.

Parameter	Description
Price	● **Yearly/Monthly**: You are billed based on the storage capacity and available duration you purchased. ● **On-demand**: You are billed based on the storage capacity you used.

Step 7 Click **OK**.

- If **Yearly/Monthly** is selected:
  a. The order confirmation page is displayed.
  b. Confirm the order and click **Pay**.
- If **On-demand** is selected:

  The capacity is successfully purchased.

  NOTE

  The backup vault will be charged after the ransomware protection is enabled. Ensure that your account balance is sufficient.

----End

5.3.2 Enabling Ransomware Prevention

Ransomware is one of the biggest cybersecurity threats today. Ransomware can intrude a server, encrypt data, and ask for ransom, causing service interruption, data leakage, or data loss. Attackers may not unlock the data even after receiving the ransom. HSS provides static and dynamic ransomware prevention. You can periodically back up server data to reduce potential losses.

If the version of the agent installed on the Linux server is 3.2.10 or later or the version of the agent installed on the Windows server is 4.0.22 or later, **ransomware prevention** is automatically enabled with the HSS premium, WTP, or container edition. Deploy bait files on servers and automatically isolate suspicious encryption processes (there is a low probability that processes are incorrectly isolated). You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Enabling Ransomware Backup**.

If the version of the agent installed on the server is not one of the preceding versions or the ransomware protection function is disabled, you can perform the operations in this section to enable ransomware protection.

Prerequisites

- You have enabled HSS premium, WTP, or container edition.
- A protection policy has been created. For details, see **Creating a Policy**.

Constraints

- Ransomware backup only supports Huawei Cloud servers.
- Only premium, WTP, and container editions support ransomware protection.

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** > **HSS**.

Step 3 Choose **Prevention** > **Ransomware Prevention**.

Step 4 Click the **Protected Servers** tab.

Step 5 In the **Ransomware Prevention Status** column of a server, click **Enable**.

You can also select multiple servers and click **Enable Ransomware Prevention** above the server list.

Step 6 In the **Enable Ransomware Prevention** dialog box, confirm the server information and select a protection policy.

Step 7 Click **OK**.

If the **Ransomware Prevention Status** of the server changes to **Enabled**, ransomware protection is enabled successfully.

----End

5.3.3 Enabling Backup

To enhance defense and reduce service loss caused by ransomware attacks, you are advised to periodically back up data on servers.

Prerequisites

- You have enabled HSS premium, WTP, or container edition.
- You have purchased a backup vault. For details, see **Purchasing a Backup Vault**.

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** > **HSS**.

Step 3 Choose **Prevention** > **Ransomware Prevention**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Protected Servers** tab.

Step 5 Select a server and click **Enable Backup**.

Step 6 In the **Enable Backup** dialog box, select a vault.

NOTE

A vault that meets the following conditions can be bound:

- The vault is in **Available** or **Locked** state.
- The backup policy is in **Enabled** state.
- The vault has backup capacity available.
- The vault is bound to fewer than 256 servers.

Step 7 Click **OK**.

----End

5.3.4 Viewing and Handling Ransomware Protection Events

After ransomware protection is enabled, if a ransomware attack event occurs on the server, the event will be recorded and displayed in the ransomware event list. You can handle the events based on your service requirements.

Prerequisites

You have enabled HSS premium, WTP, or container edition.

Constraints

- Ransomware backup only supports Huawei Cloud servers.
- After ransomware protection is enabled, you need to handle ransomware alarms and fix the vulnerabilities in your systems and middleware in a timely manner.

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** > **HSS**.

Step 3 Choose **Prevention** > **Ransomware Prevention**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Events** tab and check events.

Step 5 After confirming the severity of an event, click **Handle** in the **Operation** column of the target event to handle the event. For details about the processing modes, see **Table 5-14**.

You can also select multiple events and click **Batch Handle** above the list to handle events in batches.

Table 5-14 Alarm handling methods

Marked As	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**. **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	When manually handle an event, you can add remarks to record the details about the event.
Add to alarm whitelist	Add false alarmed items to the login whitelist. HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms. You can click **Add Rule** and configure file paths in alarm masking rules. HSS will not report the alarms matching these rules.

----End

5.3.5 Managing Ransomware Prevention Policies

You can use predefined policies, create or modify ransomware prevention policies, or change the policy associated with a server.

Constraints

Only premium, WTP, and container editions support ransomware protection.

Creating a 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** > **HSS**.

Step 3 Choose **Prevention** > **Ransomware Prevention**.

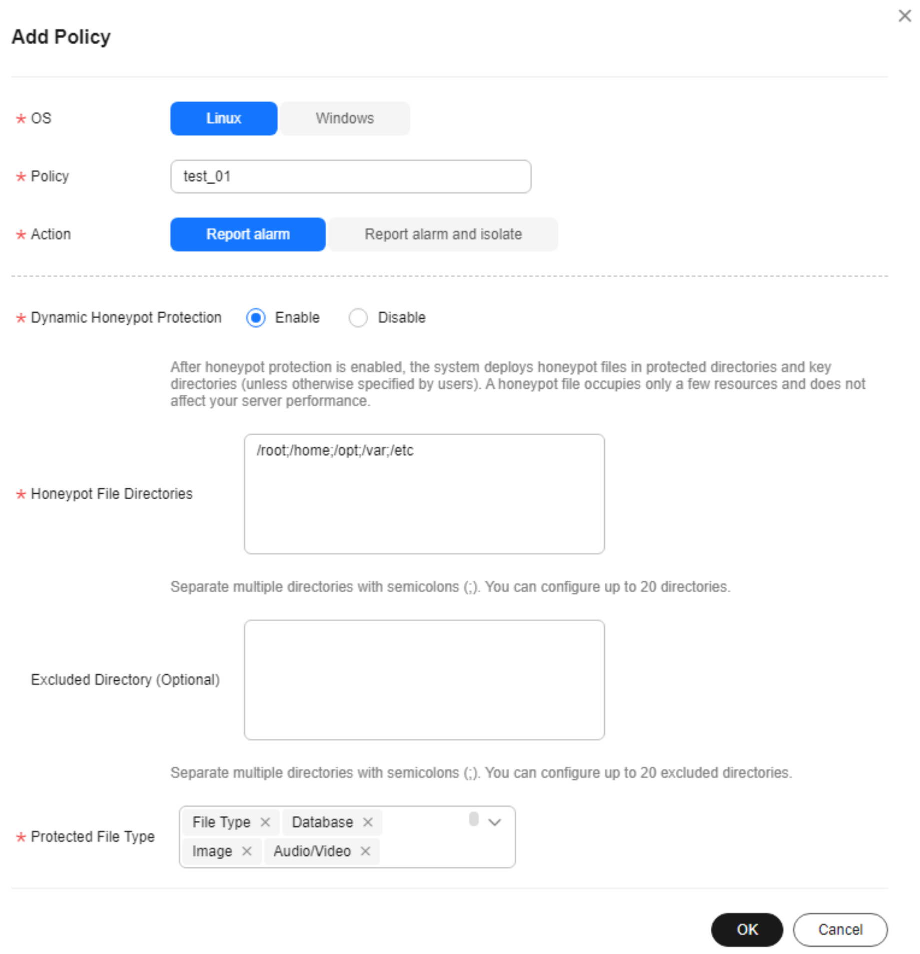
NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Policies** tab and click **Add Policy**.

Step 5 Configure policy parameters. For more information, see **Table 5-15**.

Figure 5-33 Protection policy parameters



Add Policy

* OS: Linux | Windows

* Policy: test_01

* Action: Report alarm | Report alarm and isolate

* Dynamic Honeypot Protection: ● Enable ○ Disable

After honeypot protection is enabled, the system deploys honeypot files in protected directories and key directories (unless otherwise specified by users). A honeypot file occupies only a few resources and does not affect your server performance.

* Honeypot File Directories: /root;/home;/opt;/var;/etc

Separate multiple directories with semicolons (;). You can configure up to 20 directories.

Excluded Directory (Optional):

Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.

* Protected File Type: File Type × Database × Image × Audio/Video ×

Table 5-15 Protection policy parameters

Parameter	Description	Example Value
OS	Server OS.	Linux
Policy	Policy name.	test
Action	How an event is handled. ● **Report alarm and isolate** ● **Report alarm**	Report alarm and isolate

Parameter	Description	Example Value
Dynamic Honeypot Protection	After honeypot protection is enabled, the system deploys honeypot files in protected directories and other random positions (unless otherwise specified by users). A bait file occupies a few server resources. Therefore, configure the directories that you do not want to deploy the bait file in the excluded directories. **NOTE** Currently, Linux servers support dynamic generation and deployment of honeypot files. Windows servers support only static deployment of honeypot files.	Enabled
Bait File Directories	Directory that needs to be protected by static bait (excluding subdirectories). You are advised to configure important service directories or data directories. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	Linux: **/etc** Windows: **C:\Test**
Excluded Directory (Optional)	Directory that does not need to be protected by bait files. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	Linux: **/etc/lesuo** Windows: C:\Test \ProData
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. This parameter is mandatory for Linux servers only.	Select all
(Optional) Process Whitelist	Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms. This parameter is mandatory only for Windows servers.	-

Step 6 Click **OK**.

----End

Changing a Policy

You can change the protection policy associated with a server.

Step 1 Click the **Protected Servers** tab.

Step 2 Select a server and click **Change Policy**.

Step 3 In the **Change Policy** dialog box, select a protection policy.

Step 4 Click **OK**.

----End

Modifying a Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Prevention** > **Ransomware Prevention**. Click the **Policies** tab.

Step 3 Click **Edit** in the **Operation** column of a policy. Edit the policy configurations and associated servers. For more information, see **Table 5-16**.

The following uses a Linux server as an example. On the **Protected Servers** tab, you can also click the name of the policy associated with the server to edit the policy.

Table 5-16 Protection policy parameters

Parameter	Description	Example Value
Policy	Policy name.	test
Action	How an event is handled. ● **Report alarm and isolate** ● **Report alarm**	Report alarm and isolate
Dynamic Honeypot Protection	After honeypot protection is enabled, the system deploys honeypot files in protected directories and other random positions (unless otherwise specified by users). A bait file occupies a few server resources. Therefore, configure the directories that you do not want to deploy the bait file in the excluded directories. **NOTE** Currently, Linux servers support dynamic generation and deployment of honeypot files. Windows servers support only static deployment of honeypot files.	Enabled

Parameter	Description	Example Value
Bait File Directories	Directory that needs to be protected by static bait (excluding subdirectories). You are advised to configure important service directories or data directories. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	Linux: **/etc** Windows: **C:\Test**
Excluded Directory (Optional)	Directory that does not need to be protected by bait files. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	Linux: **/etc/lesuo** Windows: C:\Test\ProData
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. This parameter is mandatory for Linux servers only.	Select all
(Optional) Process Whitelist	Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms. This parameter is mandatory only for Windows servers.	-
Associate Servers	Information about the server associated with the policy. If you want to disassociate the server (disable ransomware protection), you can delete the policy.	-

Step 4 Confirm the policy information and click **OK**.

----End

Deleting a Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Prevention** > **Ransomware Prevention**. Click the **Policies** tab.

Step 3 Click **Delete** in the **Operation** column of the target policy.

NOTE

After a policy is deleted, the associated servers are no longer protected. Before deleting a policy, you are advised to bind its associated servers to other policies.

Step 4 Confirm the policy information and click **OK**.

----End

5.3.6 Managing Server Backup

After ransomware backup is enabled, the backup vault periodically backs up your servers based on the backup policy. You can expand the vault capacity or modify the backup policy as required.

Prerequisites

Ransomware backup has been enabled. For details, see **Enabling Backup**.

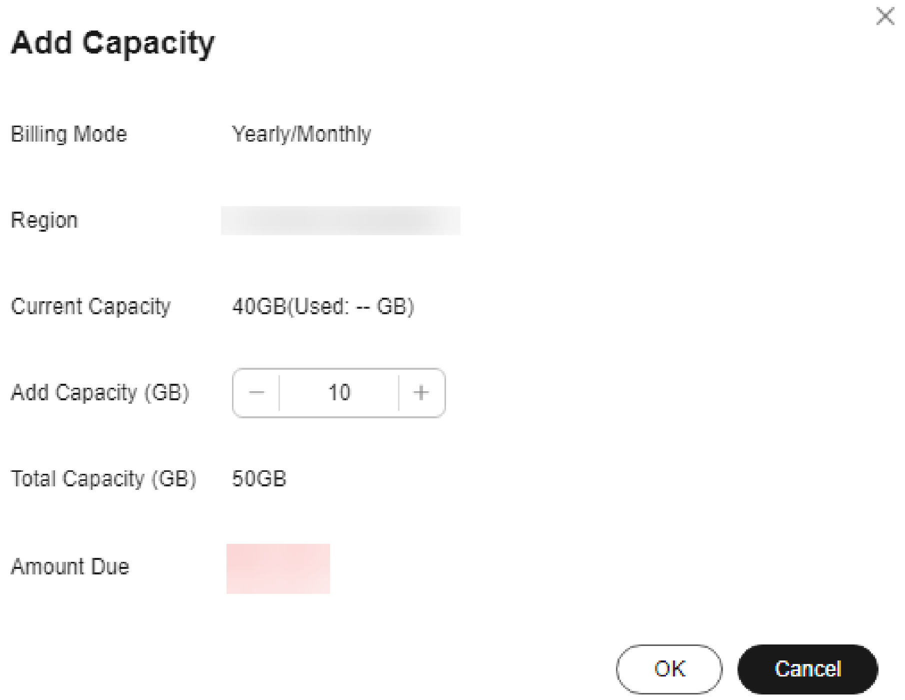
Increasing the Backup Capacity

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Prevention** > **Ransomware Prevention**. The protected server list is displayed. Click **Add Capacity** in the **Operation** column of the target server.

Step 3 In the displayed dialog box, configure the capacity.

Figure 5-34 Configuring the capacity



Add Capacity

Billing Mode: Yearly/Monthly

Region:

Current Capacity: 40GB(Used: -- GB)

Add Capacity (GB): 10

Total Capacity (GB): 50GB

Amount Due:

Step 4 If the information is correct, click **OK**. The payment page is displayed. After the payment is complete, return to the **Protected Server** tab page to view the storage capacity of the target server.

If the payment is not complete, the **Vault Status** of the target server is **Locked**. After the payment, the status becomes normal.

----End

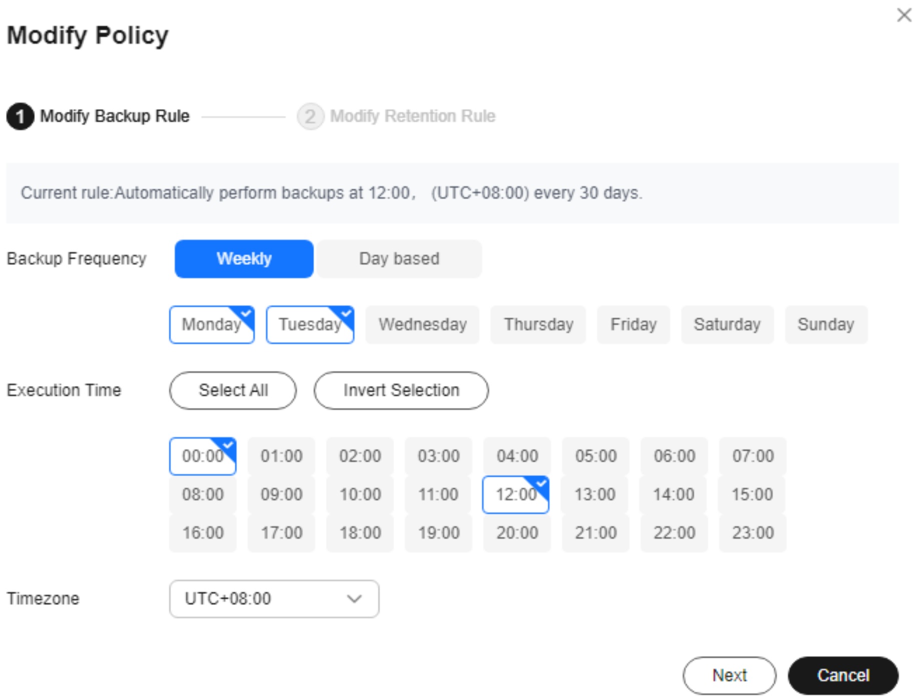
Modifying a Backup Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Prevention** > **Ransomware Prevention**. The protected server list is displayed. Click the policy name in the **Backup Policy Status** column of the target server.

Step 3 In the displayed dialog box, configure the policy. For details about the parameters, see **Policy parameters**.

Figure 5-35 Configuring a policy



Modify Policy

1 Modify Backup Rule
2 Modify Retention Rule

Current rule:Automatically perform backups at 12:00，(UTC+08:00) every 30 days.

Backup Frequency: Weekly (Monday, Tuesday)

Execution Time: 00:00, 12:00

Timezone: UTC+08:00

Table 5-17 Policy parameters

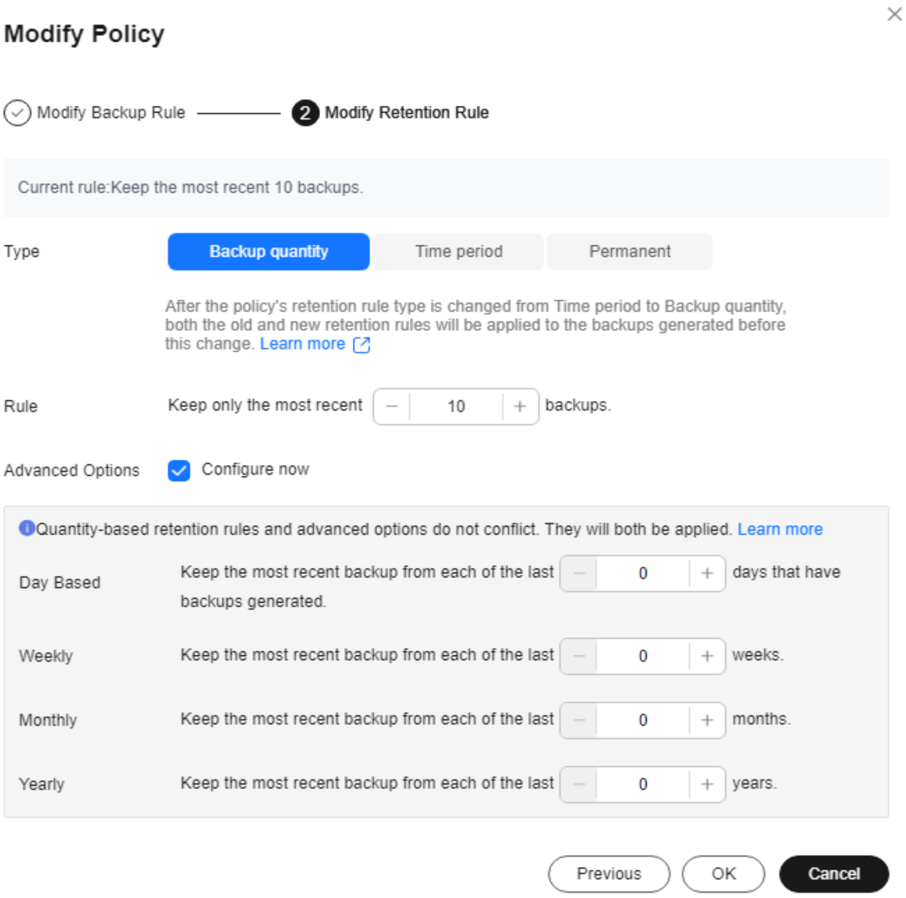
Parameter	Description	Example Value
Backup Frequency	Data can be automatically backed up on specific days in a week, or at a fixed interval. ● **Weekly**: Select one or more days in a week to back up data. ● **Day based**: The range of the backup interval is 1 to 30 days.	Weekly
Execution Time	Time when automated backup is started. **NOTE** Example of policy configurations Policy 1: Set **Backup Frequency** to **Weekly**, select **Wednesday** and **Saturday**, and set **Execution Time** to **00:00** and **13:00**. Data will be automatically backed up at 00:00 and 13:00 every Wednesday and Saturday. Policy 2: Set **Backup Frequency** to **Day based** and set the interval to two days. Set **Execution Time** to **02:00** and **14:00**. Data will be automatically backed up at 02:00 and 14:00 at an interval of two days.	00:00, 07:00
Timezone	Select the time zone of the backup time.	UTC+08:00

Step 4 Confirm the settings and click **Next**. Configure the backup retention rule.

- **Type**: **Backup quantity**

  Table 5-18 describes the parameters for configuring a backup rule.

Figure 5-36 Configuring retention rules by quantity



Modify Policy

Modify Backup Rule — 2 Modify Retention Rule

Current rule:Keep the most recent 10 backups.

Type: Backup quantity | Time period | Permanent

After the policy's retention rule type is changed from Time period to Backup quantity, both the old and new retention rules will be applied to the backups generated before this change. Learn more

Rule: Keep only the most recent 10 backups.

Advanced Options: ☑ Configure now

Quantity-based retention rules and advanced options do not conflict. They will both be applied. Learn more

Day Based: Keep the most recent backup from each of the last 0 days that have backups generated.

Weekly: Keep the most recent backup from each of the last 0 weeks.

Monthly: Keep the most recent backup from each of the last 0 months.

Yearly: Keep the most recent backup from each of the last 0 years.

Table 5-18 Parameters for data retention by quantity

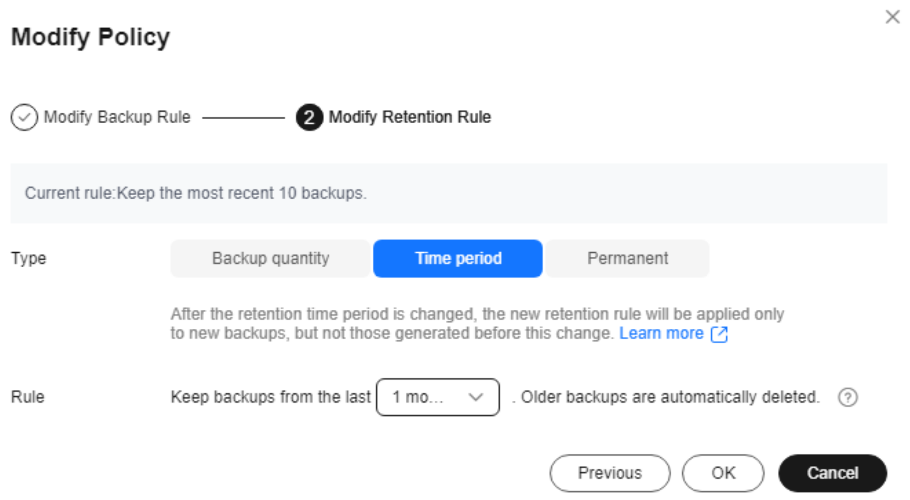
Parameter	Description	Example Value
Rule	Number of latest backups to be retained. **NOTICE** This setting takes effect no matter how you configure advanced options. For example, if the rule is configured to keep the most recent 30 backups, and **Advanced Options** are configured to keep the latest backup in the last 3 months (90 days), the latest 30 backups will be retained.	30

Parameter	Description	Example Value
(Optional) Advanced Options	You can retain the latest backup in a day, a week, a month, or a year. – Daily backup: The latest backup on each of the specified days is retained. – Weekly backup: The latest backup on each day of the specified weeks is retained. – Monthly backup: The latest backup on each day of the specified months is retained. – Yearly backup: The latest backup on each day of the specified years is retained. **NOTE** If multiple rules are configured, the rule with the longest retention period takes effect.	Keep the most recent backup from each of the last three months

- **Type**: **Time period**

  Table 5-19 describes the parameters for configuring a backup rule.

  Figure 5-37 Configuring retention rules by time period



Modify Policy

Current rule:Keep the most recent 10 backups.

Type: Backup quantity | Time period | Permanent

After the retention time period is changed, the new retention rule will be applied only to new backups, but not those generated before this change. Learn more

Rule: Keep backups from the last 1 mo... . Older backups are automatically deleted.

Table 5-19 Parameters for data retention by time period

Parameter	Description	Example Value
Rule	Select or customize a backup retention period. The system will automatically retain backups and delete old ones based on your settings. The retention period can be: – Days – 1 month – 3 months – 6 months – 1 year	3 months

- **Type**: **Permanent**

  Backup data will be permanently stored.

  NOTE

  If the **Retention Type** of a rule is changed from **Time period** to another, historical backups will still be deleted based on the **Time period** settings. For details, see **Why Does the Retention Rule Not Take Effect After Being Modified?**

Step 5 Click **OK**.

----End

5.3.7 Restoring Server Data

If your server is attacked by ransomware, you can use the backup to restore the server data to minimize the loss. Before using the backup data to restore the service data of a server, check whether the backup is available. If the backup is available, restore the key service system first.

Prerequisites

The backup function has been enabled. For details, see **Enabling Backup**.

Procedure

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Prevention** > **Ransomware Prevention**. Click the **Protected Servers** tab. In the **Operation** column of the target server, click **More** > **Restore Data**.

Step 3 In the displayed dialog box, view the information about the target server. Search for the backup data source to be restored by backup status and backup name. For details about the parameters, see **Table 5-20**.

Table 5-20 Backup data source parameters

Parameter	Description	Example Value
Backup Name	Name of a backup file.	-
Status	Backup status. It can be: ● **Available** ● **Creating** ● **Deleting** ● **Restoring** ● **Error** A backup in **Available** state can be used for restoration.	Available
Purpose	Backup purpose. It can be: ● **Periodic execution**: Data is backed up based on the backup period configured in the backup policy. ● **Ransomware protection**: Data is backed up immediately when a server is attacked by ransomware.	Periodic execution
Execution Time	Time when the data source was backed up.	-

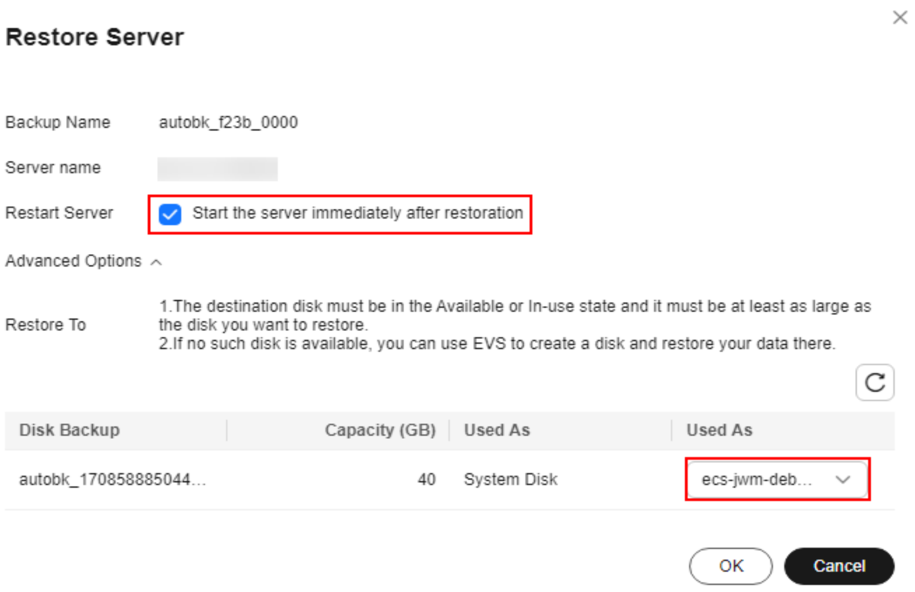
Step 4 In the **Operation** column of a backup, click **Restore Data**.

NOTE

Only a backup in the **Available** state can be restored.

Step 5 In the displayed dialog box, confirm the server information and click **OK**.

Figure 5-38 Restoring a server



Restore Server

Backup Name autobk_f23b_0000

Server name [redacted]

Restart Server ☑ Start the server immediately after restoration

Advanced Options ^

Restore To

1.The destination disk must be in the Available or In-use state and it must be at least as large as the disk you want to restore.
2.If no such disk is available, you can use EVS to create a disk and restore your data there.

Disk Backup	Capacity (GB)	Used As	Used As
autobk_170858885044...	40	System Disk	ecs-jwm-deb...

Step 6 In the **Backup Statistics** column, click the value of **Backup and Restoration Task** to view the backup and restoration progress.

----End

5.3.8 Disabling Ransomware Prevention

Scenario

You can disable ransomware protection as needed. After protection is disabled, your server may be intruded by ransomware. Exercise caution when performing this operation.

Disabling Ransomware Prevention

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** > **HSS**.

Step 3 In the navigation pane, choose **Prevention** > **Ransomware Prevention**. Click the **Protected Servers** tab.

Step 4 Click **More** > **Disable Protection** in the **Operation** column of the target server.

Step 5 Confirm the information and click **OK**.

----End

Follow-up Procedure

Disabling ransomware prevention does not stop data backup. If you no longer need backup, **dissociate your servers from CBR**. If you no longer need a backup vault, you can .

5.4 Application Process Control

5.4.1 Application Process Control Overview

HSS can learn the characteristics of application processes on servers and manage their running. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes.

Constraints

To enable application process control, the following conditions must be met:

- The HSS premium, WTP, or container edition has been enabled for your servers. For more information, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- The server agent version falls within the following scope. For more information, see **Upgrading the Agent**.
  - Linux: 3.2.7 or later
  - Windows: 4.0.19 or later

Process of Using Application Process Control

Figure 5-39 Usage process

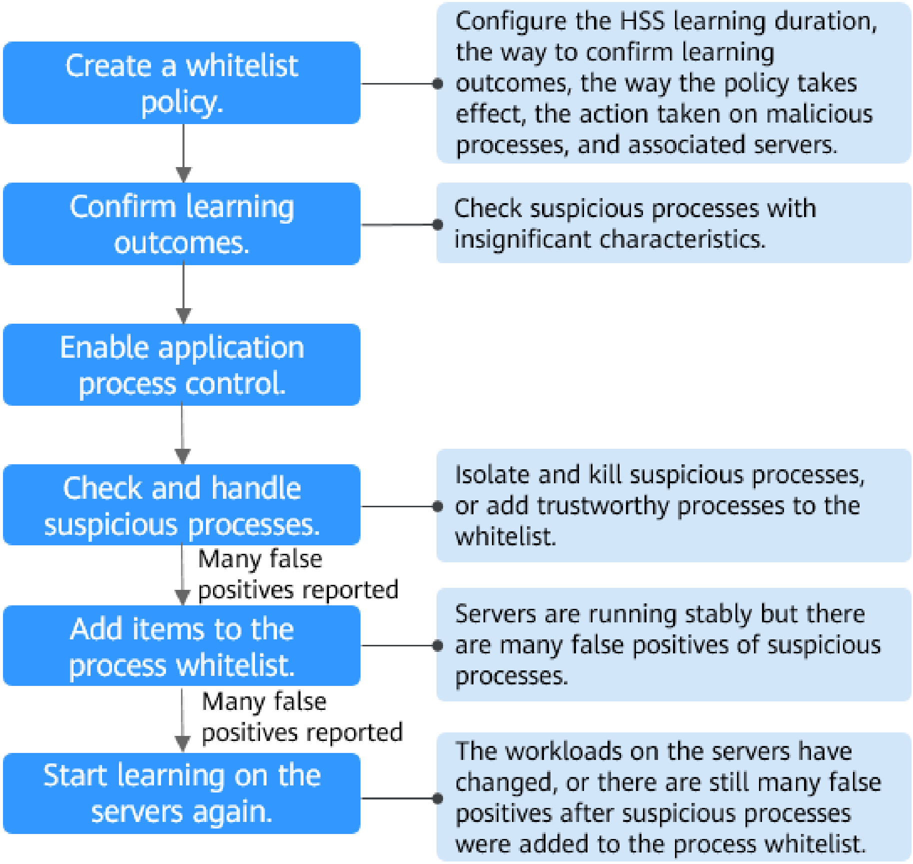

Create a whitelist policy.
Configure the HSS learning duration, the way to confirm learning outcomes, the way the policy takes effect, the action taken on malicious processes, and associated servers.
Confirm learning outcomes.
Check suspicious processes with insignificant characteristics.
Enable application process control.
Check and handle suspicious processes.
Isolate and kill suspicious processes, or add trustworthy processes to the whitelist.
Many false positives reported
Add items to the process whitelist.
Servers are running stably but there are many false positives of suspicious processes.
Many false positives reported
Start learning on the servers again.
The workloads on the servers have changed, or there are still many false positives after suspicious processes were added to the process whitelist.

Table 5-21 Process of using application process control

Operation	Description
Create a whitelist policy.	A whitelist policy specifies how HSS learns server behaviors and protect application processes. Application process protection can be enabled only for servers associated with a whitelist policy.
Confirm learning outcomes.	After the HSS learns the application processes on servers, there may be some suspicious application processes with insignificant characteristics, and HSS cannot determine whether they are malicious or trustworthy. In this case, you need to confirm the learning outcomes.
Enable application process control.	Enable application process control on the servers associated with a policy.
Check and handle suspicious processes.	HSS cannot determine whether some suspicious application processes with insignificant characteristics are trustworthy. You need to check their process details, determine whether they are trustworthy, and add them to the process whitelist or isolate and kill them.
(Optional) **Add items to the process whitelist.**	After HSS completes learning, if it regards many trustworthy application processes as suspicious, you can add these processes to the whitelist. HSS will extend the process whitelist after comparing the fingerprints of the processes it learned and those detected in asset fingerprint scans.
(Optional) **Start learning on the servers again.**	If you have added trustworthy processes to the whitelist but there are still many false positives reported, you can let HSS start learning again on the servers.

5.4.2 Creating a Whitelist Policy

Before enabling application process control, you need to create a whitelist policy and configure the HSS learning duration, the way to confirm learning outcomes, the way policy takes effect, and the action taken on suspicious or malicious processes. HSS will manage application processes based on your policies.

Procedure

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

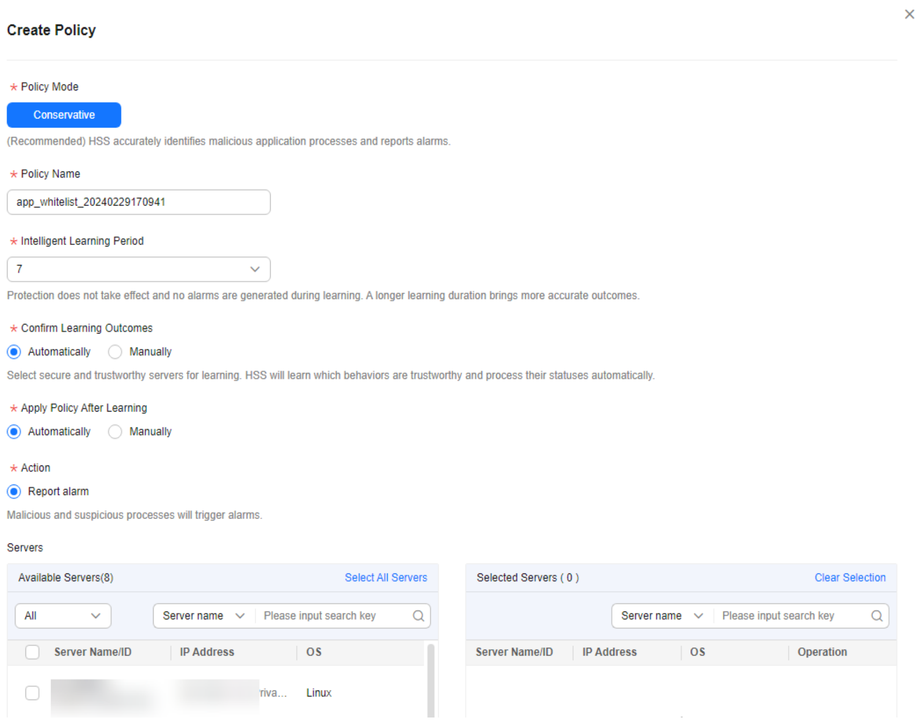
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 In the navigation tree, choose **Prevention** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab. Click **Create Policy**.

Step 5 In the **Create Policy** dialog box, configure policy parameters. For details about related parameters, see **Table 5-22**.

Figure 5-40 Creating a whitelist policy



Create Policy

* Policy Mode

Conservative

(Recommended) HSS accurately identifies malicious application processes and reports alarms.

* Policy Name

app_whitelist_20240229170941

* Intelligent Learning Period

7

Protection does not take effect and no alarms are generated during learning. A longer learning duration brings more accurate outcomes.

* Confirm Learning Outcomes

● Automatically ○ Manually

Select secure and trustworthy servers for learning. HSS will learn which behaviors are trustworthy and process their statuses automatically.

* Apply Policy After Learning

● Automatically ○ Manually

* Action

● Report alarm

Malicious and suspicious processes will trigger alarms.

Servers

Available Servers(8) Select All Servers

All | Server name | Please input search key

□	Server Name/ID	IP Address	OS
□	[redacted]	[redacted] riva...	Linux

Selected Servers (0) Clear Selection

Server name | Please input search key

Server Name/ID	IP Address	OS	Operation

Table 5-22 Whitelist policy parameters

Parameter	Description
Policy Mode	Mode of the application process control policy. The conservative mode is used by default. Trustworthy and suspicious processes are allowed to run. Alarms are generated only for malicious processes.
Policy Name	A whitelist policy name is generated by default. You are advised to set a custom name to facilitate management.
Intelligent Learning Period	Number of days that HSS learns the application processes on servers. A long learning period indicates accurate learning outcomes.

Parameter	Description
Confirm Learning Outcomes	The way to confirm suspicious processes with insignificant characteristics after HSS completes learning on the servers associated with the policy. ● **Automatically**: HSS automatically marks suspicious application processes with insignificant characteristics based on the application process signature database. ● **Manually**: Choose **Application Process Control** > **Whitelist Policies**. Click a policy name. On the policy details page, click the **Process Files** tab and filter processes in the **To be confirmed** state. Manually mark suspicious processes with insignificant characteristics.
Apply Policy After Learning	The way application process control is enabled after HSS completes learning on the servers associated with the policy. ● **Automatically**: Application process control is automatically enabled after HSS completes learning on the servers associated with the policy. ● **Manually**: Manually enable application process control as needed after HSS completes learning. For more information, see **Enabling Application Process Control**.
Action	Action taken when a malicious process is detected. Alarms are generated for malicious processes.
Servers	Servers to be protected. The agent version falls within the following scope. For details about how to upgrade the agent, see **Viewing Server Protection Status**.

Step 6 Click **OK**.

You can view the created policy and its status in the policy list.

NOTE

After a whitelist policy is created, HSS automatically starts learning the application process characteristics of the servers associated with the policy. If the policy status changes to **Learning complete but not in effect**, you can **confirm learning outcomes**.

----End

Related Operations

Editing a whitelist policy

You can modify the policy mode, action, or protected servers in a whitelist policy.

Step 1 In the row of a policy, click **Edit** in the **Operation** column.

Step 2 In the **Edit Policy** dialog box, modify parameters and click **OK**.

----End

Deleting a whitelist policy

If you no longer need HSS to provide application process control for the servers associated with a policy and do not need to retain the application process information learned by HSS, you can delete the whitelist policy. If you need to enable application process control for the servers after the deletion, HSS will need to start learning again. Exercise caution when performing this operation.

Step 1 In the row of a policy, click **Delete** in the **Operation** column.

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

----End

5.4.3 Confirming Learning Outcomes

After HSS completes learning on the servers associated with a whitelist policy, there may be some suspicious processes with insignificant characteristics that need to be confirmed. You can manually or let HSS automatically mark them as suspicious, malicious, or trustworthy processes.

You can configure how to confirm learning outcomes when creating a whitelist policy. The value of **Confirm Learning Outcomes** can be:

- **Automatically**: Suspicious processes are automatically marked based on the application process intelligence.
- **Manually**: You need to manually check and mark suspicious processes. This section describes the detailed procedure.

Prerequisites

A policy has been created and its status is **Learning complete but not in effect**. For details, see **Creating a Whitelist Policy**.

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** > **HSS**.

Step 3 In the navigation tree, choose **Prevention** > **Application Process Control**.

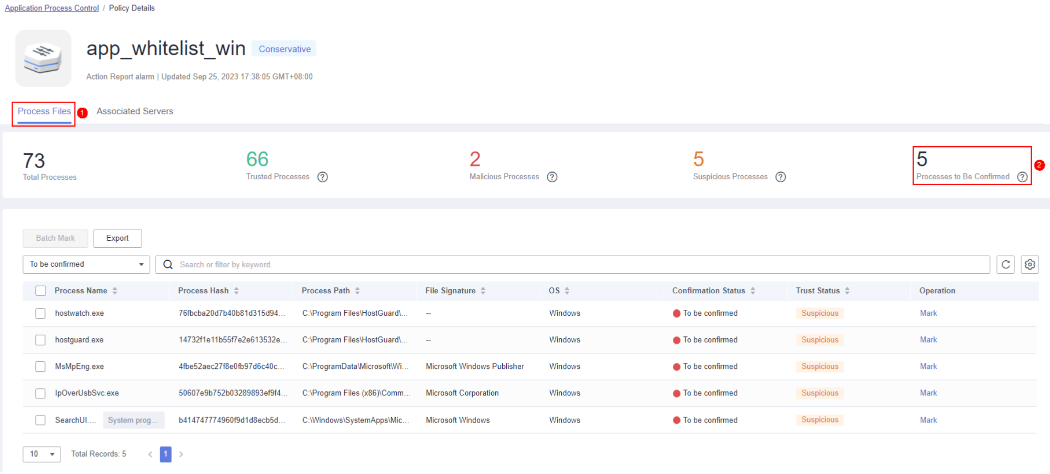
Step 4 Click the **Whitelist Policies** tab.

Step 5 Click the name of a policy whose **Policy Status** is **Learning complete but not in effect**. The **Policy Details** page is displayed.

Step 6 Click the **Process Files** tab.

Step 7 Click the number of processes to be confirmed.

Figure 5-41 Viewing processes to be confirmed



Process Name	Process Hash	Process Path	File Signature	OS	Confirmation Status	Trust Status	Operation
hostwatch.exe	76fbcba20d7b40b81d315d94...	C:\Program Files\HostGuard\...	--	Windows	● To be confirmed	Suspicious	Mark
hostguard.exe	14732f1e11b55f7e2e613532e...	C:\Program Files\HostGuard\...	--	Windows	● To be confirmed	Suspicious	Mark
MsMpEng.exe	4fbe52aec27f8e0fb97d6c40c...	C:\ProgramData\Microsoft\Wi...	Microsoft Windows Publisher	Windows	● To be confirmed	Suspicious	Mark
IpOverUsbSvc.exe	50607e9b752b03289893ef9f4...	C:\Program Files (x86)\Comm...	Microsoft Corporation	Windows	● To be confirmed	Suspicious	Mark
SearchUI.... System prog...	b414747774960f9d1d8ecb5d...	C:\Windows\SystemApps\Mic...	Microsoft Windows	Windows	● To be confirmed	Suspicious	Mark

Step 8 Check whether the application processes are trustworthy based on their names and file paths.

Step 9 In the row of a process, click **Mark** in the **Operation** column.

You can also select all application processes and click **Batch Mark** above the process list.

Step 10 In the **Mark** dialog box, set **Trust Status**.

Select **Suspicious**, **Trusted**, or **Malicious**.

Step 11 Click **OK**.

----End

5.4.4 Enabling Application Process Control

HSS can control different types of application processes on servers. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes.

You can configure how to enable application process control when creating a whitelist policy. The value of **Apply Policy After Learning** can be:

- **Automatically**: Application process control is automatically enabled after HSS completes learning on the servers associated with the policy.
- **Manually**: Manually enable application process control as needed after HSS completes learning. This section describes the detailed procedure.

Prerequisites

A whitelist policy has been created and the policy learning outcomes have been confirmed. For details, see **Creating a Whitelist Policy** and **Confirming Learning Outcomes**.

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** > **HSS**.

Step 3 In the navigation tree, choose **Prevention** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab.

Step 5 In the **Operation** column of a policy, click **Enable Protection**.

You can also select multiple policies and click **Enable Protection** above the policy list.

Step 6 In the **Enable Protection** dialog box, click **OK**.

Step 7 Check the policy status. If **Policy Status** is **Learning complete and in effect**, application protection has been enabled.

----End

5.4.5 Checking and Handling Suspicious Processes

If HSS detects suspicious processes on servers, the processes will be displayed in the suspicious process list but will not trigger alarms. HSS cannot determine whether these processes are trustworthy based on the application process characteristics. To avoid affecting services, you need to check whether the processes can be trusted, add trustworthy ones to the process whitelist, and isolate and kill the malicious ones.

Procedure

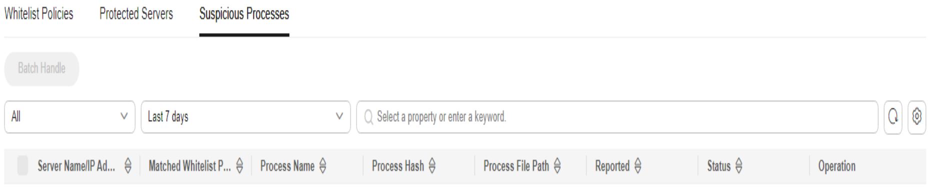
Step 1 Log in to the management console.

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

Step 3 In the navigation tree, choose **Prevention** > **Application Process Control**.

Step 4 Click the **Suspicious Processes** tab.

Figure 5-42 Viewing suspicious processes



Step 5 Determine whether a suspicious process is malicious based on its information, such as the hash value and file path.

Step 6 In the row of a process, click **Handle** in the **Operation** column.

You can also select multiple suspicious processes and click **Batch Handle** above the list.

Step 7 In the dialog box that is displayed, select an action.

Select **Add to process whitelist** or **Isolate and kill**.

Step 8 Click **OK**.

----End

5.4.6 Extending the Process Whitelist

After HSS completes learning on the servers associated a policy, if you find the learning outcomes are much fewer than the process fingerprints detected by HSS, or if too many suspicious processes are reported, you can extend the whitelist. HSS will compare the application processes it learned with and the asset fingerprints it detected, identify trustworthy processes, and add them to the process whitelist.

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** > **HSS**.

Step 3 In the navigation tree, choose **Prevention** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab.

Step 5 Click a policy name. The **Policy Details** page is displayed.

Step 6 Click the **Associated Servers** tab.

Step 7 In the row of a server, choose **More** > **Add to Whitelist** in the **Operation** column.

Step 8 Click **Compare** to compare the server process fingerprint with the application processes learned by HSS.

Step 9 Select trustworthy processes and click **Add**.

----End

5.4.7 Start Learning on Servers Again

If you have added trustworthy processes to the whitelist but there are still many false positives reported, you can let HSS start learning again on the servers.

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** > **HSS**.

Step 3 In the navigation tree, choose **Prevention** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab.

Step 5 Click a policy name. The **Policy Details** page is displayed.

Step 6 Click the **Associated Servers** tab.

Step 7 Select servers and click **Learn Again** above the list.

Step 8 In the dialog box that is displayed, click **OK**.

----End

5.4.8 Disabling Application Process Control

You can disable application process control for one or multiple servers at a time.

Disabling Protection for Servers Associated with a 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** > **HSS**.

Step 3 In the navigation tree, choose **Prevention** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab.

Step 5 Disable application process control.

- Disable protection but retain the application process characteristics learned by HSS.
  a. In the **Operation** column of a policy, click **Disable Protection**. Alternatively, select multiple policies and click **Disable** above the policy list.
  b. Click **OK**.
- Disable protection and delete the application process characteristics learned by HSS.
  a. In the row of a policy, click **Delete** in the **Operation** column.
  b. Click **OK**.

Step 6 Check the policy list.

- Disable protection but retain the application process characteristics learned by HSS.

  If the **Policy Status** of the policy is **Learning complete but not in effect**, application process control has been disabled.
- Disable protection and delete the application process characteristics learned by HSS.

  If the policy is deleted from the policy list, application process control has been disabled.

----End

Disabling Protection for a Single 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** > **HSS**.

Step 3 In the navigation tree, choose **Prevention** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab.

Step 5 Click a policy name. The **Policy Details** page is displayed.

Step 6 Click the **Associated Servers** tab.

Step 7 Disable application process control.

- Disable protection but retain the association between the server and the policy.
  1. In the **Operation** column of a policy, click **Disable Protection**. Alternatively, select multiple policies and click **Disable** above the policy list.
  2. Click **OK**.
- Disable protection and disassociate the server from the policy.

  NOTE

  To change the protection policy associated with a server, remove the server from the policy settings, and then create or edit another protection policy to associate with the server.

  1. In the row containing the desired instance, click **Delete** in the **Operation** column.
  2. Click **OK**.

Step 8 Check the server list.

- Disable protection but retain the association between the server and the policy.

  If the **Policy Status** of the server is **Learning complete but not in effect**, application process control has been disabled.
- Disable protection and disassociate the server from the policy.

  If the server is deleted from the list, application process control has been disabled.

----End

5.5 File Integrity Monitoring

You can check the statistics and details about file changes on your servers, including affected servers, file types, paths, and content.

5.5.1 Checking File Change Details

Constraints

Only premium, WTP, and container editions support file integrity-related operations.

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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Prevention** > **File Integrity Monitoring**. The file management page is displayed.

You can select an enterprise project for filtering.

Step 4 Click the **Servers** and **Modified Files** tabs to view the file change details.

Step 5 Click the server name to go to the server change details page and view the file change records of the server.

Table 5-23 Parameters about file changes

Parameter	Description	Example Value
File Name	Name of a modified file.	du
Path	Path of a modified file.	-
Change Description	Description of the change. To view the change details, hover the cursor over the change content.	**SHA2560ba0c4b5e48e55a6** is changed to **4f6079f5b37d1513**.
Type	Type of a modified file. Its value can be: ● **File**	File
Action	How a file was modified. ● Create ● Modify ● Delete	Modify
Last Modified	The last time when a file was modified.	-

----End

5.5.2 Checking Modified Files

Constraints

Only premium, WTP, and container editions support file integrity-related operations.

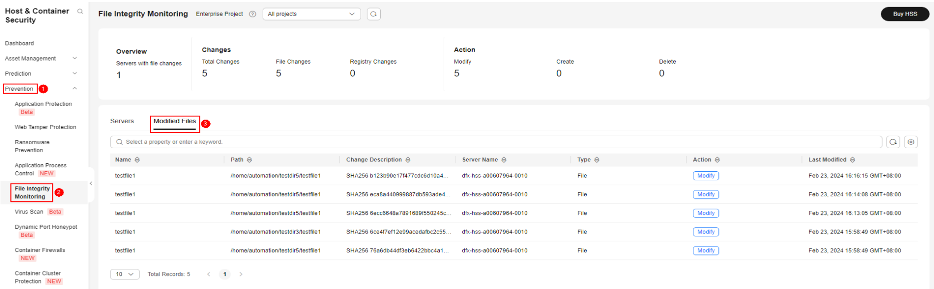
Procedure

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** > **HSS**.

Step 3 In the navigation pane, choose **Prevention** > **File Integrity Monitoring**. Click the **Monitored Files** tab. You can retain the default value for **Enterprise Project**. For details about parameters, see **Table 5-23** in **Checking File Change Details**.

Figure 5-43 Checking modified files


Host & Container Security
Dashboard
Asset Management
Prediction
Prevention
1
Application Protection Beta
Web Tamper Protection
Ransomware Prevention
Application Process Control NEW
File Integrity Monitoring
2
Virus Scan Beta
Dynamic Port Honeypot Beta
Container Firewalls NEW
Container Cluster Protection NEW
File Integrity Monitoring
Enterprise Project
All projects
Buy HSS
Servers
Modified Files
3
Select a property or enter a keyword.

Overview
Servers with file changes 1

Changes
Total Changes 5
File Changes 5
Registry Changes 0

Action
Modify 5
Create 0
Delete 0

Name	Path	Change Description	Server Name	Type	Action	Last Modified
testfile1	/home/automation/testdir5/testfile1	SHA256 b123b90e17f477cdc6d10a4...	dfx-hss-a00607964-0010	File	Modify	Feb 23, 2024 16:16:15 GMT+08:00
testfile1	/home/automation/testdir5/testfile1	SHA256 eca8a440999887db593ade4...	dfx-hss-a00607964-0010	File	Modify	Feb 23, 2024 16:14:08 GMT+08:00
testfile1	/home/automation/testdir5/testfile1	SHA256 6ecc6648a7891689f550245c...	dfx-hss-a00607964-0010	File	Modify	Feb 23, 2024 16:13:05 GMT+08:00
testfile1	/home/automation/testdir3/testfile1	SHA256 6ce4f7ef12e99acedafbc2c55...	dfx-hss-a00607964-0010	File	Modify	Feb 23, 2024 15:58:49 GMT+08:00
testfile1	/home/automation/testdir5/testfile1	SHA256 76a6db44df3eb6422bbc4a1...	dfx-hss-a00607964-0010	File	Modify	Feb 23, 2024 15:58:49 GMT+08:00

10 Total Records: 5 < 1 >

----End

5.6 Virus Scan

5.6.1 Virus Scan Overview

The function uses the virus detection engine to scan virus files on the server. The scanned file types include executable files, compressed files, script files, documents, images, and audio and video files. You can perform quick scan and full-disk scan on the server as required. You can also customize scan tasks and handle detected virus files in a timely manner to enhance the virus defense capability of the service system.

Constraints

To enable application process control, the following conditions must be met:

- The HSS professional, enterprise, premium, WTP, or container edition has been enabled for your servers. For more information, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
  - Professional edition: supports quick scanning.
  - Enterprise edition and other editions: support quick scanning, full-disk scanning, and customized scanning.
- The server agent version falls within the following scope. For more information, see **Upgrading the Agent**.
  - Linux: 3.2.9 or later
  - Windows: 4.0.20 or later
- The antivirus scan policy has been enabled on the server. For details, see **Overview**.

Process of Virus Scan

1. Scanning for Viruses
2. Viewing and Handling Viruses

5.6.2 Scanning for Viruses

Once a static virus file is started, it may become a malicious process and become a security risk of servers. Therefore, scanning static virus files is important in server security protection. HSS virus scan function can scan virus files on servers and provides the following virus scan methods:

- **Quick Scan**: Quick virus scanning tasks can save time and costs. This function scans and removes preset key system files and directories.
- **Full-disk Scan**: A time-consuming full-disk virus scanning can be implemented on servers.
- **Custom Scan**: You can customize virus scanning tasks as required.

Constraints

A virus scan uses a lot of memory, CPU, and I/O resources. Perform this operation during off-peak hours. For details about the resource usage, see **How Many CPU and Memory Resources Are Occupied by the Agent When It Performs Scans?**

Quick Scan

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** > **HSS**.

Step 3 Choose **Prevention** > **Virus Scan**. The **Virus Scan** page is displayed.

Step 4 Click **Quick Scan**. The dialog box is displayed.

Step 5 Set parameters related to the quick scan task as prompted.

- **Task Name**: You can customize a task name.
- **Select Server**: Select the server for which you want to perform quick scan.

  NOTE

  The server cannot be selected when it is in the scanning state.
- **Handling Policy**: Select the handling mode for the detected virus files.
  - **Automatic Handling**: Virus files that have been further confirmed are automatically isolated. Suspicious files are labeled with suspicious and need to be handled after manual confirmation.
  - **Manual Handling**: Alarms are displayed only for detected virus-infected files. You need to manually confirm the files before handling them.

Step 6 Click **Scan** and start the scanning task.

----End

Full-disk Scan

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** > **HSS**.

Step 3 Choose **Prevention** > **Virus Scan**. The **Virus Scan** page is displayed.

Step 4 Click **Full-disk Scan**. The dialog box is displayed.

Step 5 Set parameters related to the full-disk scan task as prompted.

- **Task Name**: You can customize a task name.
- **Select Server**: Select the server for which you want to perform full-disk scan.

  NOTE

  - The server cannot be selected when it is in the scanning state.
  - The **Full-disk Scan** function scans all disks but not network directories.
- **Handling Policy**: Select the handling mode for the detected virus files.
  - **Automatic Handling**: Virus files that have been further confirmed are automatically isolated. Suspicious files are labeled with suspicious and need to be handled after manual confirmation.
  - **Manual Handling**: Alarms are displayed only for detected virus-infected files. You need to manually confirm the files before handling them.

Step 6 Click **Scan** and start the scanning task.

----End

Custom Scan

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** > **HSS**.

Step 3 Choose **Prevention** > **Virus Scan**. The **Virus Scan** page is displayed.

Step 4 Click **Custom Scan**.

Step 5 Set the parameters of the customized antivirus policy as prompted. For details about the parameters, see **Table 1**.

Table 5-24 Custom antivirus policy parameters

Parameter	Description
Task Name	Name of a custom antivirus task.

Parameter	Description
File Type	Type of the file to be scanned. Currently, the following types of files can be scanned: ● **Executable**: executable files and dynamic link libraries (DLLs), such as .exe, .dll, and .so files. ● **Compressed**: such as .zip, .rar, and .tar ● **Script**: such as .bat, .py, and .ps1 ● **Document**: such as TXT, DOC, and PDF ● **Image**: such as BMP, JPG, and GIF ● **Audio & Video**: such as MP3, MP4, and FLV files
Directory Settings	Directory where virus-infected files need to be scanned. If this parameter is not set, full scan is performed by default. Full scan does not cover network directories.
Exclude Specified Directories	Directories that do not require virus scan.
Select Server	Servers to be scanned. Servers in the scanning state cannot be selected.
Handling Policy	Select the processing mode for the detected virus files. ● **Automatic Handling**: Virus files that have been further confirmed are automatically isolated. Suspicious files are labeled with suspicious and need to be handled after manual confirmation. ● **Manual Handling**: Alarms are displayed only for detected virus-infected files. You need to manually confirm the files before handling them.

Step 6 Click **Scan** and start the scanning task.

----End

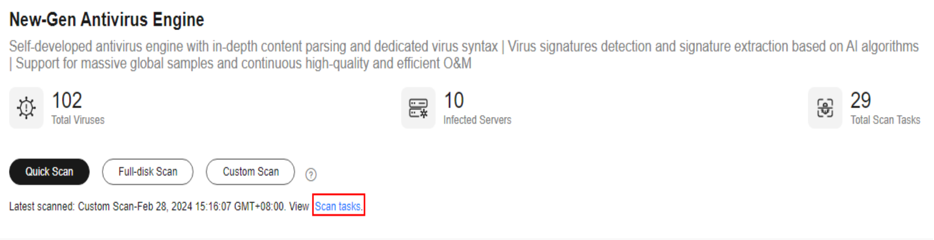
Follow-up Procedure

- View the execution status of a scan job

  a. On the **Virus Scan** page, click the **Scan tasks** to view the execution status of virus scan tasks.

     To stop an ongoing scan task, click **Cancel** in the **Operation** column of the target scan task.

Figure 5-44 Viewing scan tasks



New-Gen Antivirus Engine

Self-developed antivirus engine with in-depth content parsing and dedicated virus syntax | Virus signatures detection and signature extraction based on AI algorithms | Support for massive global samples and continuous high-quality and efficient O&M

102 Total Viruses

10 Infected Servers

29 Total Scan Tasks

Latest scanned: Custom Scan-Feb 28, 2024 15:16:07 GMT+08:00. View Scan tasks.

b. Click ⌄ to view the scan status and number of scanned files of each server.

   Click **Cancel** in the **Operation** column of the target server to stop scanning the server.

- View and handle viruses

  After a virus scan task is complete, you can manually handle the detected virus files based on service requirements. For details, see **Viewing and Handling Viruses**.

5.6.3 Viewing and Handling Viruses

After the virus scanning is complete, the system handles the infected files based on the handling policy selected. The handling policies are as follows:

- **Automatic Handling**: Virus files that have been further confirmed are automatically isolated. Suspicious files are labeled with suspicious and need to be handled after manual confirmation.
- **Manual Handling**: Alarms are generated only for detected infected files. You need to manually confirm the files before handling them.

The section describes how to view and manually handle infected files.

Prerequisites

A virus scanning task has been executed. For details, see **Scanning for Viruses**.

Viewing and Handling Viruses

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** > **HSS**.

Step 3 Choose **Prevention** > **Virus Scan**. The **Virus Scan** page is displayed.

Step 4 View the scanned virus files.

Step 5 In the **Operation** column of a virus file, click **Handle**.

You can also select multiple virus files and click **Batch Handle** above the list to handle them in batches.

Step 6 In the **Handle Infected Files** dialog box, select a virus-infected file handling method. For details about the processing modes, see **Virus-infected file handling methods**.

Table 5-25 Virus-infected file handling methods

Parameter	Description
Mark as handled	You can manually handle the virus-infected file on the server.
Ignore	Ignore the virus-infected file alarm. If the virus-infected file alarm event occurs again, HSS generates an alarm.
Add to alarm whitelist	If you confirm that the virus file is falsely reported, you can add it to the alarm whitelist. After a file is added to whitelist, HSS will not generate alarms for the file.
Manually isolating files	After a file is isolated, the read/write operation cannot be performed on the virus-infected file. Isolated files are added to the **Isolated Files** and cannot harm your server. You can restore or delete isolated files as required. For details, see **Isolated Files**.

Step 7 Click **OK**.

After the alarm is handled, the status of the virus file alarm event changes to **Handled**. You can view the handling records on the historical handling records page. For details, see **Viewing the Handling History**.

----End

Exporting Virus-infected File Alarms

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** > **HSS**.

Step 3 Choose **Prevention** > **Virus Scan**. The **Virus Scan** page is displayed.

Step 4 Above the virus-infected file alarm event list, click **Export** to export all virus-infected file alarm events to the local PC.

Step 5 In the displayed dialog box, click **OK**.

Step 6 View the export status in the upper part of the virus scan page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

5.6.4 Managing Isolated Files

Isolated files are added to the **Isolated Files** and cannot harm your server. You can also refer to this section to restore or delete isolated files as required.

Restoring Isolated Files

If you want to de-isolate an isolated file, you can restore it by referring to the following steps.

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** > **HSS**.

Step 3 Choose **Prevention** > **Virus Scan**. The **Virus Scan** page is displayed.

Step 4 Click **Isolated Files** in the upper right corner of the page. The dialog box is displayed.

Step 5 Click **Restore** in the **Operation** column of the list. The dialog box is displayed.

Step 6 Click **OK**.

NOTE

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

----End

Deleting Isolated Files

If you want to permanently delete an isolated file, you can perform the deletion operation by referring to the following steps.

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** > **HSS**.

Step 3 Choose **Prevention** > **Virus Scan**. The **Virus Scan** page is displayed.

Step 4 Click **Isolated Files** in the upper right corner of the page. The dialog box is displayed.

Step 5 Click **Delete** in the **Operation** column of the list. The dialog box is displayed.

To delete isolated files in batches, select multiple isolated files and click **Delete** in the upper left corner of the list.

Step 6 Click **OK**.

NOTE

Deleted isolated files cannot be restored. Exercise caution when performing this operation.

----End

5.7 Dynamic Port Honeypot

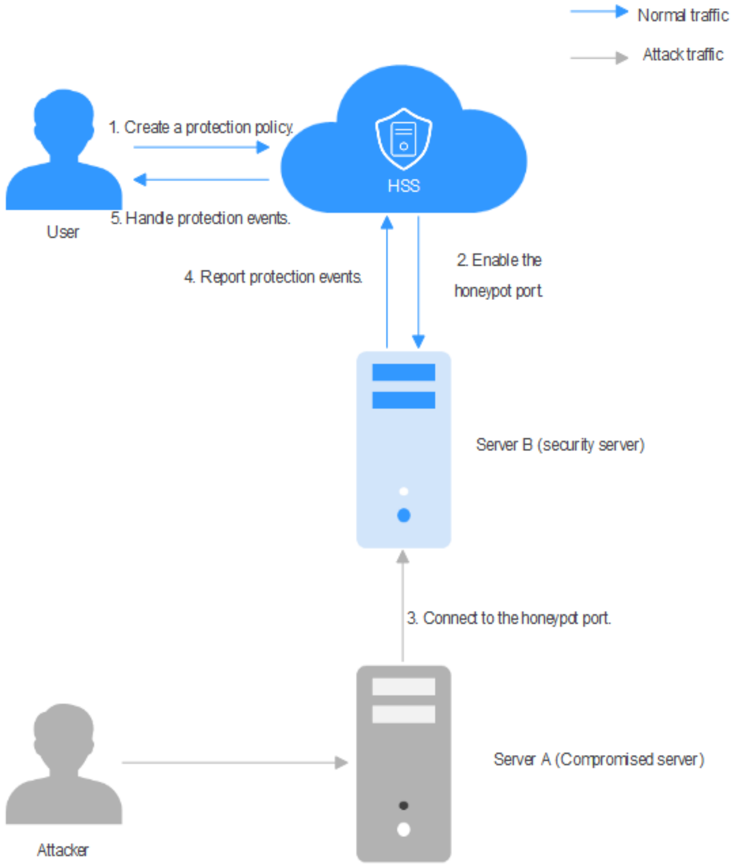
5.7.1 Dynamic Port Honeypot Overview

What is Dynamic Port Honeypot?

The dynamic port honeypot function is a deception trap. It uses a real port as a bait port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect real resources of the user.

You can enable the dynamic port honeypot using recommended ports or user-defined ports to deceive compromised servers and reduce the risk of resources intrusion.

Figure 5-45 Conceptual diagram of dynamic port honeypot protection


Normal traffic
Attack traffic
1. Create a protection policy.
HSS
User
5. Handle protection events.
4. Report protection events.
2. Enable the honeypot port
Server B (security server)
3. Connect to the honeypot port.
Server A (Compromised server)
Attacker

How Do I Use Dynamic Port Honeypot?

Figure 5-46 shows the process of using the dynamic port honeypot.

Figure 5-46 Process of using the dynamic port honeypot

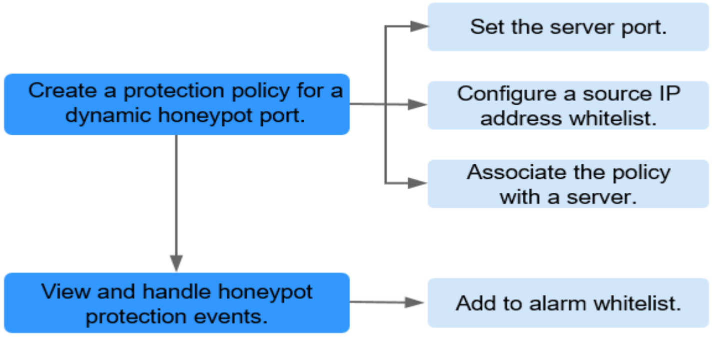

Create a protection policy for a dynamic honeypot port.
Set the server port.
Configure a source IP address whitelist.
Associate the policy with a server.
View and handle honeypot protection events.
Add to alarm whitelist.

Table 5-26 Process of using the dynamic port honeypot

Operation	Description
Creating a Protection Policy for the Dynamic Honeypot Port	Enable the server port of dynamic port function, configure the source IP address whitelist, and bind the protected server.
Viewing and Handling Honeypot Protection Events	The dynamic port honeypot function reports an alarm when a potentially compromised server proactively connects to a honeypot port. You can handle the alarm based on service requirements.

Constraints and Limitations

- The HSS premium, WTP, or container edition has been enabled for your servers. For more information, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- The server agent version falls within the following scope. For more information, see **Upgrading the Agent**.
  - Linux: 3.2.10 or later.
  - Windows: 4.0.22 or later.
- A maximum of 10 honeypot ports can be added to a server.
- A honeypot port can be bound to only one protocol. Both TCP and TCP6 are supported.

5.7.2 Creating a Protection Policy for a Dynamic Honeypot Port

Scenario

The dynamic port honeypot function uses a real port as a honeypot port to induce attackers to access the network. Therefore, when enabling dynamic port honeypot protection, you need to create a protection policy to add a server port as a honeypot port and bind it to the server for protection.

This chapter describes how to create a dynamic port honeypot protection policy.

Constraints and Limitations

- A maximum of 10 honeypot ports can be added to a server.
- A honeypot port can be bound to only one protocol. Both TCP and TCP6 are supported.

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** > **HSS**.

Step 3 Choose **Prevention** > **Dynamic Port Honeypot**. The **Dynamic Port Honeypot** page is displayed.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 On the **Servers** tab, click **Create a Protection Policy**. The dialog box is displayed.

Step 6 Create a protection policy as prompted.

1. Configure the policy and click **Next**. For details about related parameters, see **Table 5-27**

Table 5-27 Parameters for creating a protection policy

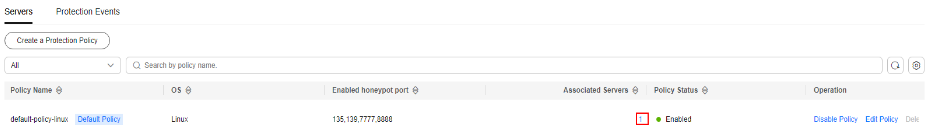
Parameter	Description
Policy Name	You can retain the default name or enter a name that is easy to identify.
OS Type	Select an OS type of a server to which you want to add the dynamic port honeypot function.

Parameter	Description
Protected Port	Select a server port that implements the dynamic port honeypot function. – **Recommended Port**: For Linux, common Windows ports are recommended. For Windows, common Linux ports are recommended. – **Custom Port**: You can add custom ports or delete some recommended ports as required. **NOTE** Ensure that the port to be added is not occupied by other services. If the port is occupied, the dynamic port honeypot function fails to be enabled.
(Optional) Source IP address whitelist	By default, the servers that proactively connect to the dynamic honeypot port are compromised intranet servers. Once a suspicious connection behavior is detected, an alarm is reported. Therefore, if a trusted server may connect to the port, you are advised to add the IP address to the source IP address whitelist.

2. Select the target server and click **Save and Enable**.

Step 7 In the **Associated Servers** column of the created target policy, click the value. The dialog box is displayed.

Figure 5-47 Associate servers



Policy Name	OS	Enabled honeypot port	Associated Servers	Policy Status	Operation
default-policy-linux Default Policy	Linux	135,139,7777,8888	1	● Enabled	Disable Policy Edit Policy Dele

Step 8 In the **Port Status** column of the associated server, check the port status.

To enable the port again, click the **Edit Policy** to select server, and then bind the server. For details about how to edit a policy, see **Editing a Policy**.

----End

FAQs

What can I do if the port fails to be enabled?

- Possible cause 1: The port is occupied by other services.

  Solution: Add other idle ports by editing the policy.

- Possible cause 2: System resources are insufficient.

  Solution: Free up some system resources, click the **Edit Policy** to select server, and then bind the server. For details about how to edit a policy, see **Editing a Policy**.

5.7.3 Viewing and Handling Honeypot Protection Events

Scenario

By default, the servers that proactively connect to the dynamic honeypot port are compromised intranet servers. Once a suspicious connection behavior is detected, an alarm is reported.

This chapter describes how to view and handle these alarms and events.

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** > **HSS**.

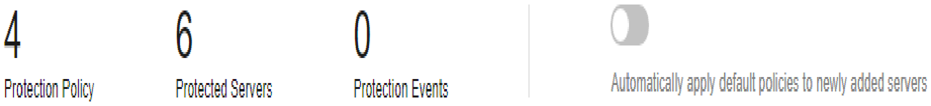
Step 3 Choose **Prevention** > **Dynamic Port Honeypot**. The **Dynamic Port Honeypot** page is displayed.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Under the introductions, view the protection overview.

- You can view the number of protection policies, protected servers, and protection events.
- You can enable the **Automatically apply default policies to newly add servers**. If ● is displayed, the function is enabled.

Figure 5-48 Protection information overview



4 Protection Policy

6 Protected Servers

0 Protection Events

Automatically apply default policies to newly added servers

Step 6 Click the **Protection Events** tab to view honeypot protection events. For details about the parameters in the event list, see **Table 5-28**.

Table 5-28 Parameters in the event list

Parameter	Description
Alarm Name	The name of an alarm event. Click an alarm name to view the details. For details, see **Table 5-30**.
Alert Severity	Alarm threat level. Honeypot protection events are classified into the following two levels: ● High risk: The remote server connects to the honeypot port for multiple times. ● Medium risk: The remote server is connected to the honeypot port.

Parameter	Description
Alarm Summary	Summary of alarm events. Based on the information, you can learn about the server that may be compromised and the connection between the server and the port.
Affected Asset	Dynamic port server connected to the compromised server.
Alarm Reported	Time when an alarm occurred.
Status	Alarm handling status, which can be **Handled** or **To be handled**.
Operation	You can handle alarm events.

Step 7 After confirming the alarm information, click **Handle** in the **Operation** column of the event whose **Status** is **To be handled**. The **Handle Alarm** dialog box is displayed.

If you need to handle multiple alarm events in batches, click **Batch Handle** in the upper left corner of the list.

Step 8 Select a solution. For details about the solution, see **Table 5-29**.

Table 5-29 Parameters for handling alarm events

Parameter	Description
Action	● Ignore: Ignore the alarm event. The alarm is still generated when the next threat event occurs. ● Manually handling: You can manually isolate ports for the compromised server. ● Add to alarm whitelist: Add the trusted server that triggers an alarm to the whitelist so that no alarm will be generated when similar threat events occur.
Batch handling	If you need to handle the same alarm event at the same time, you can select the parameter.
Remarks (Optional)	To facilitate identification of the current processing, supplementary description can be provided.

Step 9 Click **OK**.

----End

Alarm Details Parameters

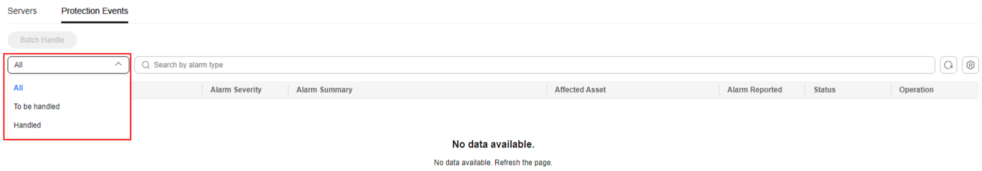
For details about the parameters on the alarm details, see **Table 5-30**.

Table 5-30 Alarm details parameters

Parameter	Description
Intelligence Engine	Detection engines used by HSS, including the virus detection engine, AI detection engine, and malicious intelligence detection engine.
Attack Status	Status of the current threat.
First Occurred	Time when an attack alarm is generated for the first time
Alarm ID	Unique ID of an alarm
ATT&CK Phase	Attack model used by attackers in each phase.
Last Occurred	Time when an attack alarm is generated for the last time
Alarm Information	Detailed information about an alarm, including the alarm description, alarm summary, affected assets, and handling suggestions.
Forensics	The dynamic port honeypot function checks the network forensics information of the attack source.
Similar Alarms	Alarms that are similar to the current alarm event. You can handle the alarm according to the handling method of the similar alarms.

Filtering Events in Different Handling Statuses

Select an event in the target status from the drop-down list.



No data available.

No data available. Refresh the page.

5.7.4 Managing Dynamic Port Honeypot Protection Policies

Scenario

After a policy is created, you can manage the policy based on your protection requirements.

- **Disabling a policy**: Disable the dynamic port honeypot function temporarily.
- **Enabling a policy**: Enable a disabled function of dynamic port honeypot.

- **Editing a policy**: Modify the protection policy information of dynamic port honeypot, for example, adding or deleting ports, and unbinding or binding servers.
- **Deleting a policy**: Delete the dynamic port honeypot protection policy and disable the function.

Constraints and Limitations

The default policy cannot be deleted.

Disabling a 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** > **HSS**.

Step 3 Choose **Prevention** > **Dynamic Port Honeypot**. The **Dynamic Port Honeypot** page is displayed.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the row containing the target policy, click **Disable Policy** in the **Operation** column. The dialog box is displayed.

Step 6 Confirm the information and click **OK**.

----End

Enabling a 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** > **HSS**.

Step 3 Choose **Prevention** > **Dynamic Port Honeypot**. The **Dynamic Port Honeypot** page is displayed.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the row containing the target policy, click **Enable Policy** in the **Operation** column. The dialog box is displayed.

Step 6 Confirm the information and click **OK**.

----End

Editing a 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** > **HSS**.

Step 3 Choose **Prevention** > **Dynamic Port Honeypot**. The **Dynamic Port Honeypot** page is displayed.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the row containing the target policy, click **Edit Policy** in the **Operation** column. The dialog box is displayed.

Step 6 Configure a policy.

You can modify the policy name, protected port, and source IP address whitelist.

Step 7 Click **Next**.

Step 8 Select a server to be bound.

Step 9 Click **OK**.

----End

Delete a 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** > **HSS**.

Step 3 Choose **Prevention** > **Dynamic Port Honeypot**. The **Dynamic Port Honeypot** page is displayed.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the row containing the target policy, click **Delete Policy** in the **Operation** column. The dialog box is displayed.

Step 6 Ensure that all information is correct and click **OK**.

----End

5.7.5 Managing Associated Servers

Scenario

For servers associated with a protection policy, you can **switch the protection policy** for servers or **unbind the protection policy** from the servers.

Changing a 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** > **HSS**.

Step 3 Choose **Prevention** > **Dynamic Port Honeypot**. The **Dynamic Port Honeypot** page is displayed.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the **Associated Servers** column of the target policy, click the value. The dialog box is displayed.

Step 6 Click **Change Policy** in the **Operation** column. The **Change Policy** dialog box is displayed.

To switch protection policies for multiple servers, select all target servers and click **Change Policy** in the upper left corner of the list.

Step 7 Select a protection policy as prompted.

Step 8 Click **OK**.

----End

Unbinding a 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** > **HSS**.

Step 3 Choose **Prevention** > **Dynamic Port Honeypot**. The **Dynamic Port Honeypot** page is displayed.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the **Associated Servers** column of the target policy, click the value. The dialog box is displayed.

Step 6 Click **Unbind** in the **Operation** column. The **Unbind** dialog box is displayed.

To unbind multiple servers, select all target servers and click **Unbind** in the upper left corner of the list.

Step 7 Confirm the information and click **OK**.

----End

5.8 Container Firewalls

5.8.1 Container Firewall Overview

A container firewall controls and intercepts network traffic inside and outside a container cluster to prevent malicious access and attacks.

Constraints

- Only the HSS container edition supports this function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.

- To operate resource objects in a cluster, you need to obtain either of the following operation permissions:
  - IAM permissions: Tenant Administrator or CCE Administrator.
  - Namespace permissions (authorized by Kubernetes RBAC): O&M permissions. For details about how to configure permissions, see **Configuring namespace permissions**.

How It Works

A container firewall controls the access scope of source and destination containers based on the access policies for pods and servers, blocking internal and external malicious accesses and attacks.

Protected Cluster Type

Clusters purchased in CCE.

Related Operations

- **Creating a Network Policy (for a Cluster Using the Container Tunnel Network Model)**
- **Creating a Security Group Rule (VPC Network Model Cluster)**
- **Creating a Security Group Policy (Cloud Native Network 2.0)**

5.8.2 Creating a Network Policy (for a Cluster Using the Container Tunnel Network Model)

You can configure network policies to limit the access traffic to the pods in a cluster using the container tunnel network model. If no network policies are configured, all the inbound and outbound traffic of the pods in a namespace are allowed by default.

This section describes how to create a network policy for a cluster using the container tunnel network model.

Constraints

- Only clusters that use the tunnel network model support network policies. Network policies are classified into the following types:
  - Inbound rules, which are supported by all CCE cluster versions.
  - Outbound rules, which are supported only by CCE clusters in version 1.23 and later.
- Network isolation is not supported for IPv6 addresses.

Creating a Network Policy from YAML

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prevention** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on CCE.

The task takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Step 6 Click **Manage Policy** in the **Operation** column of a cluster using the container tunnel network model.

Step 7 Click **Create from YAML** above the policy list.

Step 8 On the YAML creation page, enter content or click **Import**.

An example of a network policy created from YAML is as follows:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:                  # The rule takes effect for pods with the role=db label.
    matchLabels:
      role: db
  policyTypes:
    - Ingress
    - Egress
  ingress:                      # Ingress rule
    - from:
        - namespaceSelector: # Only namespaces with project=myproject can be accessed.
            matchLabels:
              project: myproject
        - podSelector:              # Only the traffic from the pods with the role=frontend label is allowed.
            matchLabels:
              role: frontend
      ports                     # Only TCP can be used to access port 6379.
        - protocol: TCP
          port: 6379
  egress:                       # Egress rule
    - to:
        - ipBlock:                 #Only the 10.0.0.0/24 network segment of the destination object can be accessed.
            cidr: 10.0.0.0/24
      ports:                    # Only TCP can be used to access port 6379 of the destination object.
        - protocol: TCP
          port: 6379
```

Step 9 Click **OK**.

----End

Creating a Network Policy on the GUI

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prevention** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on CCE.

The task takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Step 6 Click **Manage Policy** in the **Operation** column of a cluster using the container tunnel network model.

Step 7 Click **Create Network Policy** above the network policy list.

- **Policy Name**: Enter a network policy name.
- **Namespace**: Select a namespace for the network policy.
- **Selector**: Enter a key and a value to set the pod to be associated, and click **Add**. You can also click **Reference Workload Label** to reference the label of an existing workload. If this parameter is not specified, all pods in the namespace are associated by default.
- Inbound rule: Click **Add Rule** in the **Inbound Rules** area. For more information, see **Table 5-31**.

Table 5-31 Adding an inbound rule

Parameter	Description
Protocol & Port	Enter the inbound protocol type and port number of the pods to be associated. Currently, TCP and UDP are supported. If this parameter is not specified, all access traffic is allowed.
Source Namespace	Select a namespace whose objects can be accessed. If this parameter is not specified, access to the objects that belong to the same namespace as the current policy is allowed.
Source Pod Label	Select a label. Pods with this label can be accessed. If this parameter is not specified, all pods in the namespace can be accessed.

- Outbound rule: Click **Add Rule** in the **Outbound Rules** area. For more information, see **Table 5-32**.

Table 5-32 Adding an outbound rule

Parameter	Description
Protocol & Port	Enter the port and protocol of destination objects. If this parameter is not specified, access is not limited.

Parameter	Description
Destination CIDR Block	Configure CIDR blocks. This parameter allows requests to be routed to a specified CIDR block (and not to the exception CIDR blocks). Separate the destination and exception CIDR blocks by vertical bars (|), and separate multiple exception CIDR blocks by commas (,). For example, 172.17.0.0/16|172.17.1.0/24,172.17.2.0/24 indicates that 172.17.0.0/16 is accessible, but not for 172.17.1.0/24 or 172.17.2.0/24.
Destination Namespace	Namespace where the destination object is located. If not specified, the object belongs to the same namespace as the current policy.
Destination Pod Label	Select a label. Pods with this label can be accessed. If this parameter is not specified, all pods in the namespace can be accessed.

Step 8 Click **OK**.

----End

5.8.3 Creating a Security Group Rule (VPC Network Model Cluster)

For clusters using the VPC network model, you can configure security group rules to limit the traffic that accesses the servers where containers are deployed. If no security group rules are configured, all incoming and outgoing traffic of the servers is allowed by default.

This section describes how to create a security group rule for a cluster using the VPC network model.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prevention** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on CCE.

The task takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Step 6 Click **Manage Policy** in the **Operation** column of a cluster using the VPC network model.

Step 7 In the **Operation** column of a node, click **Configure Policy**.

Step 8 In the displayed dialog box, click **OK** to go to the cloud server console.

Step 9 Click the **Security Groups** tab and view security group rules.

Step 10 Click **Manage Rule**. The security group page is displayed.

Step 11 Configure inbound and outbound rules.

For details, see **Adding a Security Group Rule**.

----End

5.8.4 Creating a Security Group Policy (Cloud Native Network 2.0)

For clusters using the cloud native network 2.0 model, you can configure security group policies to limit the traffic that accesses the servers where containers are deployed. If no security group policies are configured, all incoming and outgoing traffic of the servers is allowed by default.

This chapter describes how to create a security group policy for a cluster using the cloud native network 2.0 model.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prevention** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on CCE.

The task takes about 1 to 2 minutes. Wait for a while and click ↻ in the upper right corner of the list to refresh and view the latest data.

Step 6 Click **Manage Policy** in the **Operation** column of a cluster using the cloud native network 2.0 model.

Step 7 Click **Create** above the policy list. The **Create a Security Group Policy** dialog box is displayed.

Step 8 Enter the policy information as prompted. For details about related parameters, see **Table 5-33**.

Table 5-33 Parameters for creating a security group policy

Parameter	Description
Policy	Enter a policy name.
Namespace	A namespace to be selected.
Workload Type	Select a load type. The following types are supported: ● Deployment ● StatefulSets ● DaemonSets
Workload	Select the target workload.
Associate a Security Group	Select a security group to be associated. Each policy can be associated with a maximum of five groups. The existing security groups in the list are those you have created in the VPC service. To create a security group, click **Create a Security Group** to go to the VPC console. For details, see **Create a Security Group**.

Step 9 After entering the policy information, click **OK**.

----End

5.8.5 Managing Network Policies (for a Cluster Using the Container Tunnel Network Model)

You can modify or delete the policies of a cluster using the container tunnel network model.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prevention** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Manage Policy** in the **Operation** column of a cluster using the VPC network model.

Step 6 Click **Synchronize** above the network policy list.

The task takes about 1 to 2 minutes. Wait for a while and click ↻ in the upper right corner of the list to refresh and view the latest data.

Step 7 Manage policies as needed.

- Modifying a policy
  - In the **Operation** column of a policy, click **Edit YAML**. On the YAML page, modify the YAML content and click **OK**.
  - In the **Operation** column of a policy, click **Update**. Modify the network policy information and click **OK**.
- Deleting a policy
  - In the **Operation** column of a policy, click **Delete**. In the confirmation dialog box, click **OK**.
  - Select one or multiple policies and click **Delete** above the policy list. In the displayed dialog box, click **OK**.

----End

5.8.6 Managing Security Group Rules (VPC Network Model Cluster)

You can modify the rule or delete unnecessary rules by following the instructions provided in this section.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prevention** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Manage Policy** in the **Operation** column of a cluster using the VPC network model.

Step 6 Click **Synchronize** above the node list to synchronize node information.

The task takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Step 7 In the **Operation** column of a node, click **Configure Policy**.

Step 8 In the displayed dialog box, click **OK** to go to the cloud server console.

Step 9 Click the **Security Groups** tab and view security group rules.

Step 10 Click **Manage Rule**. The security group page is displayed.

Step 11 Click a rule tab and manage rules as needed.

- Modifying a rule

  In the **Operation** column of a rule, click **Modify**. Modify the rule and click **OK**.
- Deleting a rule

In the **Operation** column of a rule, click **Delete**. In the confirmation dialog box, click **OK**.

----End

5.8.7 Managing Security Group Policy (Cloud Native Network 2.0)

You can modify or delete the policies of a cluster using the cloud native network 2.0 model by referring to this chapter.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Prevention** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Manage Policy** in the **Operation** column of a cluster using the cloud native network 2.0 model.

Step 6 Click **Synchronize** above the policy list to synchronize cluster policy information.

The task takes about 1 to 2 minutes. Wait for a while and click ↻ in the upper right corner of the list to refresh and view the latest data.

Step 7 Select the operation to be performed on the policy.

- View policy content.

  In the **Operation** column of a policy, click **View YAML**. In the displayed dialog box, you can select **YAML** or **JSON** to view the policy details. Click **Download** in the upper left corner of the dialog box.

- Update policy content.

  a. Locate a target policy and click **Update** in the **Operation** column. The **Update a Security Group Policy** dialog box is displayed.

  b. Add or delete an associated security group.

  c. Click **OK**.

- Delete a policy.

  a. Locate a target policy and click **Delete** in the **Operation** column. The **Delete Policy** dialog box is displayed.

  b. Ensure that all information is correct and click **OK**.

----End

5.9 Container Cluster Protection

5.9.1 Container Cluster Protection Overview

HSS can check for non-compliance baseline issues, vulnerabilities, and malicious files when a container image is started and report alarms on or block container startup that has not been unauthorized or may incur high risks.

You can configure container cluster protection policies to block images with vulnerabilities, malicious files, non-compliant baselines, or other threats, hardening cluster security.

Constraints

To enable container cluster protection, the following conditions must be met:

- You have purchased a CCE cluster in version 1.20 or later.
- The HSS container edition has been enabled for container node servers. For more information, see **Purchasing HSS Quotas**.
- The server agent version falls within the following scope. For more information, see **Upgrading the Agent**.
  - Linux: 3.2.7 or later
  - Windows: 4.0.19 or later
- To operate resource objects in a cluster, you need to obtain either of the following operation permissions:
  - IAM permissions: Tenant Administrator or CCE Administrator.
  - Namespace permissions (authorized by Kubernetes RBAC): O&M permissions. For details about how to configure permissions, see **Configuring namespace permissions**.

Process of Using Container Cluster Protection

Figure 5-49 Usage process

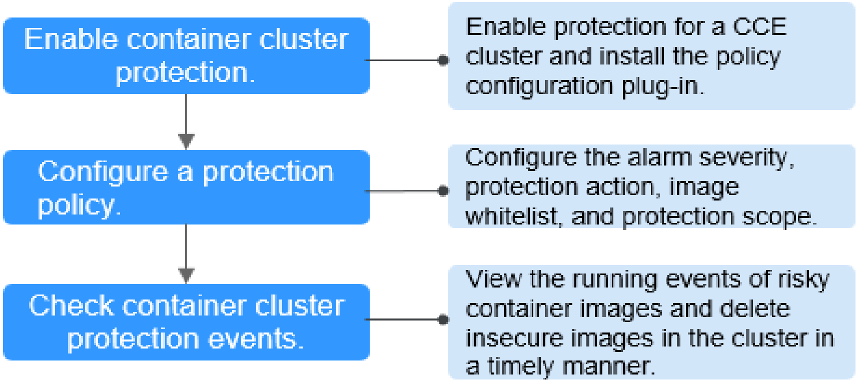

Enable container cluster protection.
Enable protection for a CCE cluster and install the policy configuration plug-in.
Configure a protection policy.
Configure the alarm severity, protection action, image whitelist, and protection scope.
Check container cluster protection events.
View the running events of risky container images and delete insecure images in the cluster in a timely manner.

Table 5-34 Process of using container cluster protection

Operation	Description
Enable container cluster protection.	Enable protection for a CCE cluster to protect its workloads and critical data security. When protection is enabled, HSS automatically installs the policy management plug-in on the cluster.
Configure a protection policy.	Configure the severity of baseline, vulnerability, and malicious file risks that trigger alarms; container cluster protection scope; image whitelist; and actions to be taken on alarms.
Check container cluster protection events.	On the HSS console, you can view unauthorized or high-risk container image running events that are reported or blocked, and check and clear insecure container images in a timely manner.

5.9.2 Enabling Container Cluster Protection

Container cluster protection can detect risks in baselines, vulnerabilities, and malicious files; and can report alarms on or block insecure container images. You can enable protection to enhance cluster defense and protect containers.

Constraints

After container cluster protection is enabled, you need to configure a policy to make the protection take effect. For more information, see **Configuring a Container Cluster Protection Policy**.

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** > **HSS**.

Step 3 In the navigation pane, choose **Prevention** > **Container Cluster Protection**.

Step 4 Click the **Protected Clusters** tab.

Step 5 Click **Synchronize** to synchronize CCE clusters.

Step 6 In the **Operation** column of a cluster, click **Enable Protection**.

To enable protection for clusters in batches, select clusters and click **Enable Protection** in the upper left corner of the cluster list.

NOTICE

- After container cluster protection is enabled for a cluster, the policy management plug-in will be installed in the cluster and occupy some cluster resources.
- When enabling protection for a container cluster, do not perform any operation on the cluster. Otherwise, protection will fail to be enabled.

Step 7 Click **OK**.

If the **Protection Status** of the container cluster is **Enabled but not configured**, it indicates protection has been configured for the cluster and the policy management plug-in has been installed, but HSS has not started to protect your cluster. In this case, you need to configure a protection policy. For more information, see **Configuring a Container Cluster Protection Policy**.

----End

5.9.3 Configuring a Container Cluster Protection Policy

You can configure container cluster protection policies to specify the level of risks (unsafe baselines, vulnerabilities, or malicious files) that trigger alarms, cluster protection scope, image whitelist, and the actions taken on an alarm.

Creating a 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** > **HSS**.

Step 3 In the navigation pane, choose **Prevention** > **Container Cluster Protection**.

Step 4 Click the **Protection Policies** tab and click **Create Policy**.

Step 5 Configure parameters in the **Create Policy** dialog box.

1. Configure a protection policy. The following table describes the parameters.

Table 5-35 Container cluster protection policy parameters

Parameter	Description
Policy Template	Select a policy template.
Policy Name	User-defined policy name.
Policy Description	Description about the policy.

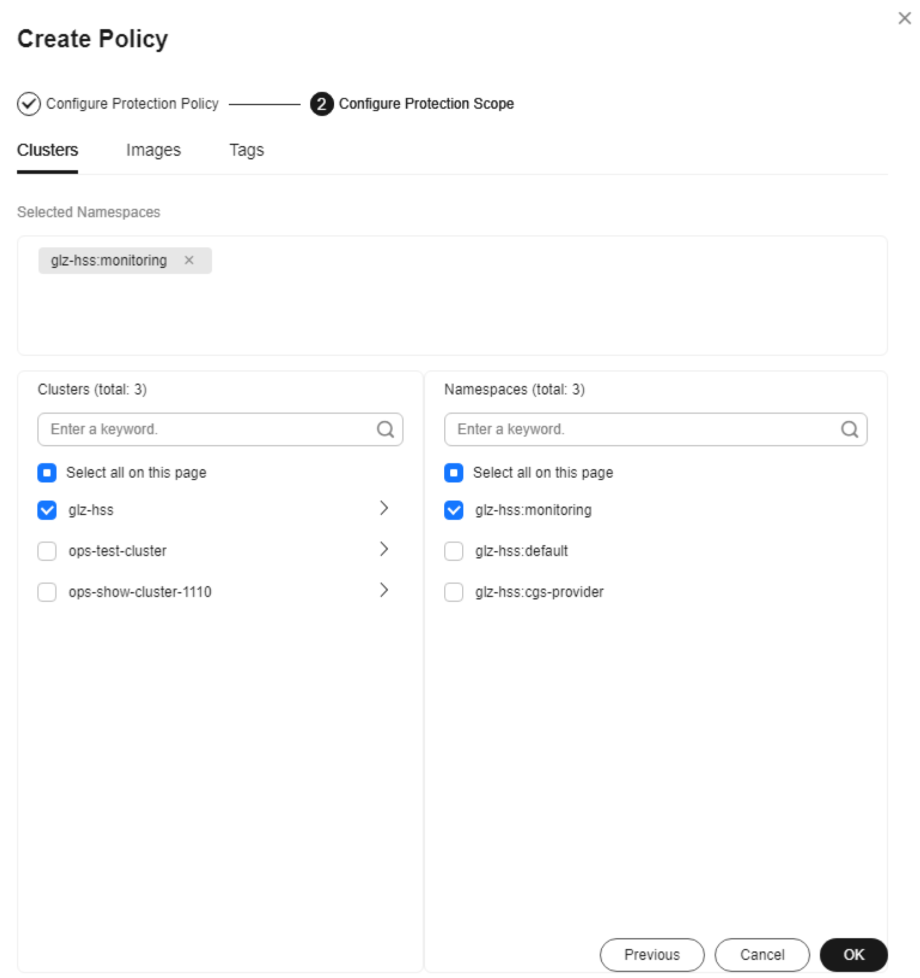
Parameter	Description
Block Unscanned Images	Whether to block images that have not been scanned using the HSS container image security function. – : disable – : enabled
Alarm Policy	Alarm policy type. – **Baseline** – **Vulnerability** – **Malicious script**
Risk Level	Risk level that triggers an alarm. – **High** – **Medium** – **Low**
Baseline Item	Configure unsafe baseline items. If an image to be started contains any of these items, HSS will take specified actions immediately.
Vulnerability Item	Configure vulnerabilities. If an image to be started contains any of these vulnerabilities, HSS will take specified actions immediately.
Malicious Sample	Configure malicious samples. If an image to be started contains any of these samples, HSS will take specified actions immediately.
Action	Action taken by HSS if it detects that an image to be started contains specified unsafe baseline items, vulnerabilities, or malicious scripts. – **Alarm**: Generate an event whose **Action** is **Alarm** on the **Protection Events** tab of the **Container Cluster Protection** page. – **Block**: Block an unsafe image and generate an event whose **Action** is **Block** on the **Protection Events** tab of the **Container Cluster Protection** page. – **Allow**: Generate an event whose **Action** is **Allow** on the **Protection Events** tab of the **Container Cluster Protection** page.

Parameter	Description
Add to Whitelist	Images to be added to the whitelist. Enter values in *ImageName*:*ImageVersion* format. An image name can contain only numbers, letters, underscores (_), hyphens (-), and periods (.). Each image name occupies a separate line. Example: – A single image **image:1.0** – Multiple images **image1:1.0** **image2:1.0** **NOTICE** Exercise caution when performing this operation. HSS does not check whitelisted images when they are started.

2. Click **Next**.
3. Configure protection scope.

   Configure the protection scope of clusters, images, and tags.

Figure 5-50 Configuring protection scope



Create Policy

✓ Configure Protection Policy —— 2 Configure Protection Scope

Clusters | Images | Tags

Selected Namespaces

glz-hss:monitoring ×

Clusters (total: 3)

Enter a keyword.

■ Select all on this page

☑ glz-hss >

□ ops-test-cluster >

□ ops-show-cluster-1110 >

Namespaces (total: 3)

Enter a keyword.

■ Select all on this page

☑ glz-hss:monitoring

□ glz-hss:default

□ glz-hss:cgs-provider

Step 6 Click **OK**.

You can view the new protection policy in the policy list.

----End

Editing or Deleting a Cluster Protection Policy

Step 1 Choose **Container Cluster Protection** and click the **Protection Policies** tab.

Step 2 In the **Operation** column of a policy, click a button as required.

- **Edit**: Modify a protection policy.
- **Delete**: Delete a protection policy.

NOTICE

After a policy is deleted, the container clusters associated with it will no be protected. Exercise caution when performing this operation.

Step 3 Click **OK**.

----End

5.9.4 Checking Container Cluster Protection Events

HSS detects risks and displays security events in the protection event list. This section describes how to check the events.

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** > **HSS**.

Step 3 In the navigation pane, choose **Prevention** > **Container Cluster Protection**.

Step 4 Click the **Protection Events** tab and check events in the cluster.

Step 5 Click an alarm name to view affected resources.

----End

5.9.5 Disabling Container Cluster Protection

If you no longer need HSS to protect your container clusters, you can disable container cluster protection.

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** > **HSS**.

Step 3 In the navigation pane, choose **Prevention** > **Container Cluster Protection**.

Step 4 Click the **Protected Clusters** tab.

Step 5 In the **Operation** column of a cluster, click **Disable Protection**.

To disable protection for clusters in batches, select clusters and click **Disable Protection** in the upper left corner of the cluster list.

Step 6 In the dialog box that is displayed, determine whether to select the **Delete policy plug-in of the cluster** check box.

- If you select it, container cluster protection policies and the policy configuration plug-in will be deleted. If you enable protection again, you will need to install the policy configuration plug-in and configure protection policies again.
- If you deselect it, container cluster protection policies will be deleted but the policy configuration plug-in will be retained. If you enable protection again, you only need to configure protection policies. If you want to delete the policy configuration plug-in later, repeat the preceding steps to disable protection and select **Delete policy plug-in of the cluster**.

Step 7 Click **OK**.

If you did not select **Delete policy plug-in of the cluster** and the **Protection Status** of the cluster changes to **Enabled but not configured**, it indicates protection has been disabled.

If you selected **Delete policy plug-in of the cluster** and the **Protection Status** of the cluster changes to **Unprotected**, it indicates protection has been disabled.

----End

FAQ

If the cluster network is abnormal or the plug-in is working, you will probably fail to uninstall the plug-in on the HSS console. In this case, you can refer to the content below: **What Do I Do If the Container Cluster Protection Plug-in Fails to Be Uninstalled?**

6 Intrusion Detection

6.1 Alarms

6.1.1 HSS Alarms

6.1.1.1 Server Alarms

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

NOTE

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

Constraints

Servers that are not protected by HSS do not support alarm-related operations.

Supported Alarms and Events

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
Malware	Unclassified malware	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.	×	√	√	√	√	Linux and Windows	√	√	√
	Viruses	Detect viruses in server assets, report alarms, and support automatic or manual viruses isolation and killing based on the alarms.	×	√	√	√	√	Linux and Windows	√	√	√

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Worms	Detect and kill worms on servers and report alarms.	×	√	√	√	√	Linux and Windows	√	√	√
	Trojans	Detect and remove Trojan and viruses on servers and report alarms.	×	√	√	√	√	Linux and Windows	√	√	√
	Botnets	Detect and kill botnets on servers and report alarms.	×	√	√	√	√	Linux and Windows	√	√	√

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Backdoors	Detect backdoors in servers and reports alarms.	×	√	√	√	√	Linux and Windows	√	√	×
	Rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.	×	√	√	√	√	Linux	√	×	×
	Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.	×	×	×	√	√	Linux and Windows	√	√ (Partially supported)	√ (Partially supported)

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Hacker tools	Detect and kill hacker tools on servers and reports alarms.	×	×	√	√	√	Linux and Windows	√	√	×
	Web shells	Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. You can configure the web shell detection rule in the **Web Shell Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands. You need to add a protected directory in policy management. For details, see **Web Shell Detection**.	×	√	√	√	√	Linux and Windows	√	√	×
	Mining	Detect, scan, and remove mining software on servers, and report alarms.	×	√	√	√	√	Linux and Windows	√	√	√

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
Vulnerability Exploits	Remote code execution	Detect and report alarms on server intrusions that exploit vulnerabilities in real time.	×	×	√	√	√	Linux and Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms.	×	√	√	√	√	Linux	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms.	×	√	√	√	√	Linux	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms.	×	√	√	√	√	Linux	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
Abnormal System Behavior	Reverse shells	Monitor user process behaviors in real time to report alarms on and block 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 and automatic blocking in the **Malicious File Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands. You can also configure automatic blocking of reverse shells in the **HIPS Detection** rule on the **Policies** page.	×	√	√	√	√	Linux	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	File privilege escalations	Detect file privilege escalation behaviors and generate alarms.	×	√	√	√	√	Linux	√	×	×
	Process privilege escalations	Detect the privilege escalation operations of the following processes and generate alarms: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities	×	√	√	√	√	Linux	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Important file changes	Monitor important system files (such as ls, ps, login, and top) in real time and generate alarms if these files are modified. For details about the monitored paths, see **Monitored Important File Paths**. HSS reports all the changes on important files, regardless of whether the changes are performed manually or by processes.	×	√	√	√	√	Linux	√	×	×
	File/Directory changes	Monitor system files and directories in real time and generate alarms if such files are created, deleted, moved, or if their attributes or content are modified.	×	√	√	√	√	Linux and Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Abnormal process behaviors	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	×	×	√	√	√	Linux and Windows	√	√ (Partially supported)	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	High-risk command executions	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.	×	√	√	√	√	Linux and Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	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. You can configure the abnormal shell detection rule in the **Malicious File Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands.	×	√	√	√	√	Linux	√	×	×
	Suspicious crontab tasks	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.	×	×	×	√	√	Linux and Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	System protection disabling	Detect the preparations for ransomware encryption: Disable the Windows defender real-time protection function through the registry. Once the function is disabled, an alarm is reported immediately.	×	×	√	√	√	Windows	√	×	×
	Backup deletion	Detect the preparations for ransomware encryption: Delete backup files or files in the **Backup** folder. Once backup deletion is detected, an alarm is reported immediately.	×	×	√	√	√	Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Suspicious registry operations	Detect operations such as disabling the system firewall through the registry and using the ransomware **Stop** to modify the registry and write specific strings in the registry. An alarm is reported immediately when such operations are detected.	×	×	√	√	√	Windows	√	×	×
	System log deletions	An alarm is generated when a command or tool is used to clear system logs.	×	×	√	√	√	Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Suspicious command executions	● Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. ● Detect suspicious remote command execution.	×	×	√	√	√	Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Suspicious process execution	Detect and report alarms on unauthenticated or unauthorized application processes.	×	×	√	√	√	Linux and Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Suspicious process file access	Detect and report alarms on the unauthenticated or unauthorized application processes accessing specific directories.	×	×	√	√	√	Linux and Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
Abnormal User Behavior	Brute-force attacks	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. The default blocking duration is 12 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.	√	√	√	√	√	Linux and Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	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. ● 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, an alarm will be triggered. ● Trigger an alarm if a user logs in by a brute-force attack.	√	√	√	√	√	Linux and Windows	√	×	×
	Invalid accounts	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.	×	√	√	√	√	Linux and Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	User account added	Detect the commands used to create hidden accounts. Hidden accounts cannot be found in the user interaction interface or be queried by commands.	×	×	√	√	√	Windows	√	×	×
	Password theft	Detect the abnormal obtaining of system accounts and password hashes on servers and report alarms.	×	×	√	√	√	Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
Abnormal Network Access	Suspicious download request	An alarm is generated when a suspicious HTTP request that uses system tools to download programs is detected.	×	×	√	√	√	Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Suspicious HTTP requests	An alarm is generated when a suspicious HTTP request that uses a system tool or process to execute a remote hosting script is detected.	×	×	√	√	√	Windows	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
	Abnormal outbound connection	Report alarms on suspicious IP addresses that initiate outbound connections.	×	√	√	√	√	Linux	√	×	×
	Port forwarding	Report alarms on port forwarding performed using suspicious tools.	×	√	√	√	√	Linux	√	×	×

Event Type	Alarm Name	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Manual Isolation and Killing	Automatic Isolation and Killing
Reconnaissance	Portscan	Detect scanning or sniffing on specified ports and report alarms.	×	×	×	√	√	Linux	×	×	×
	Hostscan	Detect the network scan activities based on server rules (including ICMP, ARP, and nbtscan) and report alarms.	×	×	×	√	√	Linux	√	×	×

Monitored Important File Paths

Type	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login

Type	Linux
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

6.1.1.2 Viewing Server Alarms

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 urgent alarms, total alarms, servers with alarms, blocked IP addresses, and isolated files.

The **Events** page displays the alarm events generated in the last 30 days. You can manually handle the alarmed items.

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

NOTE

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

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 **Viewing a Policy Group**.
- Other detection items cannot be manually disabled.
- Servers that are not protected by HSS do not support operations related to alarms and events.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Detection** > **Alarms** and click **Server Alarms**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Table 6-1 Alarm statistics

Parameter	Description
Enterprise Project	Select an enterprise project and view alarm details by enterprise project.
Time range	You can select a fixed period or customize a time range to search for alarms. Only alarms generated within 30 days can be queried. The options are as follows: ● Last 24 hours ● Last 3 days ● Last 7 days ● Last 30 days
Urgent Alarms	Number of urgent alarms that need to be handled.
Total Alarms	Total number of alarms on your assets.
Affected Servers	Number of servers for which alarms are generated. When checking alarms generated in the last 24 hours, you can click the number of servers to go to the **Servers & Quota** page and check the corresponding servers.
Handled Alarms	Number of handled alarms.

Parameter	Description
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 name, attack source IP address, login type, blocking status, number of blocks, blocking start time, and the latest blocking time. 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** ● The agent of Linux 3.2.10 or later supports IPv6 interception. The agent of a version earlier than Linux 3.2.10 supports TCP Wrapper interception, but does not support IPv6 interception using IPTables. ● After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address. ● A maximum of 10,000 IP addresses can be blocked for each type of software. If your Linux server does not support ipset, a maximum of 50 IP addresses can be clocked for MySQL and vsftp. If your Linux server does not support ipset or hosts.deny, a maximum of 50 IP addresses can be blocked for SSH.
Isolated Files	HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** 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 Check alarms on your assets.

In the **Alarms to Be Handled** area, you can select an alarm type and an ATT&CK phase to view the alarms of the selected type.

ATT&CK attack phase tags are also displayed below alarm names. For more information, see **Table 6-2**.

NOTE

Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a framework that helps organizations understand the cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle.

Table 6-2 ATT&CK phases

ATT&CK Phase	Description
Reconnaissance	Attackers seek vulnerabilities in your system or network.
Initial Access	Attacker try to enter your system or network.

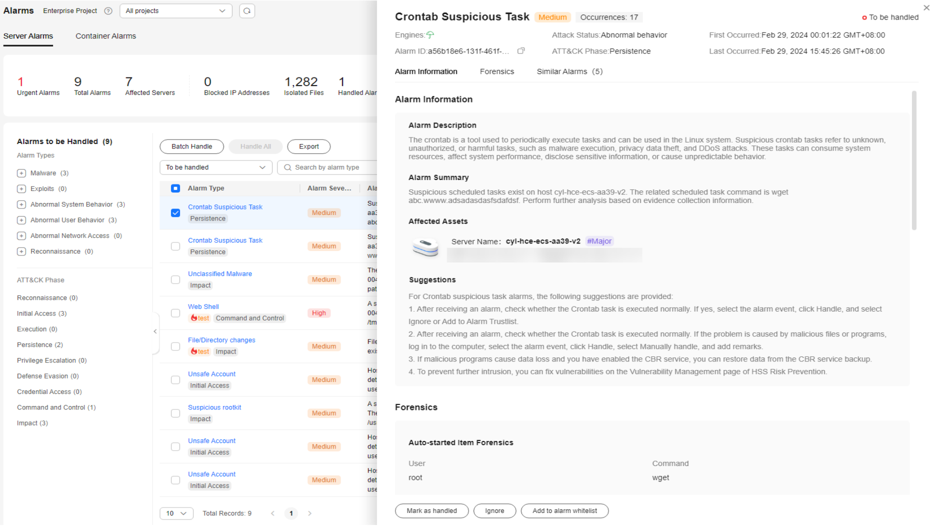
ATT&CK Phase	Description
Execution	Attackers try to run malicious code.
Persistence	Attackers try to maintain their foothold.
Privilege Escalation	Attackers try to obtain higher permissions.
Defense Evasion	Attackers try to avoid being detected.
Credential Access	Attackers try to steal account names and passwords.
Command and Control	Attackers try to communicate with compromised machines to control them.
Impact	Attackers try to manipulate, interrupt, or destroy your system or data.

Step 5 Click an alarm name to view its details. **Table 6-3** describes the alarm parameters.

NOTE

You can download the alarm source files of certain malware to your local PC for analysis. The password for decompressing the files is **unlock**.

Figure 6-1 Alarm details



Alarm Type	Alarm Seve...
☑ Crontab Suspicious Task Persistence	Medium
□ Crontab Suspicious Task Persistence	Medium
□ Unclassified Malware Impact	Medium
□ Web Shell test Command and Control	High
□ File/Directory changes test Impact	Medium
□ Unsafe Account Initial Access	Medium
□ Suspicious rootkit Impact	Medium
□ Unsafe Account Initial Access	Medium
□ Unsafe Account Initial Access	Medium

Crontab Suspicious Task Medium Occurrences: 17 ○ To be handled

Engines:
Attack Status:Abnormal behavior
First Occurred:Feb 29, 2024 00:01:22 GMT+08:00
Alarm ID:a56b18e6-131f-461f-...
ATT&CK Phase:Persistence
Last Occurred:Feb 29, 2024 15:45:26 GMT+08:00

Alarm Information

Alarm Description

The crontab is a tool used to periodically execute tasks and can be used in the Linux system. Suspicious crontab tasks refer to unknown, unauthorized, or harmful tasks, such as malware execution, privacy data theft, and DDoS attacks. These tasks can consume system resources, affect system performance, disclose sensitive information, or cause unpredictable behavior.

Alarm Summary

Suspicious scheduled tasks exist on host cyl-hce-ecs-aa39-v2. The related scheduled task command is wget abc.wwww.adsadasdasfsdafdsf. Perform further analysis based on evidence collection information.

Affected Assets

Server Name: cyl-hce-ecs-aa39-v2 #Major
[redacted]

Suggestions

For Crontab suspicious task alarms, the following suggestions are provided:
1. After receiving an alarm, check whether the Crontab task is executed normally. If yes, select the alarm event, click Handle, and select Ignore or Add to Alarm Trustlist.
2. After receiving an alarm, check whether the Crontab task is executed normally. If the problem is caused by malicious files or programs, log in to the computer, select the alarm event, click Handle, select Manually handle, and add remarks.
3. If malicious programs cause data loss and you have enabled the CBR service, you can restore data from the CBR service backup.
4. To prevent further intrusion, you can fix vulnerabilities on the Vulnerability Management page of HSS Risk Prevention.

Forensics

Auto-started Item Forensics

User	Command
root	wget

Table 6-3 Alarm detail parameters

Parameter	Description
Intelligence Engine	Detection engines used by HSS, including the virus detection engine, AI detection engine, and malicious intelligence detection engine.
Attack Status	Status of the current threat.

Parameter	Description
First Occurred	Time when an attack alarm is generated for the first time
Alarm ID	Unique ID of an alarm
ATT&CK Phase	For details about the attack technology models used by attackers in each phase, see **Table 6-2**.
Last Occurred	Time when an attack alarm is generated for the last time
Alarm Information	Detailed information about an alarm, including the alarm description, alarm summary, affected assets, and handling suggestions.

Parameter	Description
Forensics	HSS investigates information such as the attack triggering path or virus type based on the alarm type, helping you quickly trace and locate the attack source. ● **Process Tree**: If an alarm event contains process information, you can check the process ID, process file path, process command line, process startup time, and process file hash on the **Forensics** tab page. You can locate malicious processes based on such information. ● **File Forensics**: If an alarm event contains file information, you can check the file path and file hash on the **Forensics** tab page. You can locate the files based on the such information. ● Network Forensics: If an alarm event contains file information, the network forensics information is displayed on the **Forensics** tab page. Network forensics information includes the local IP address, local port, remote IP address, remote port, and protocol. You can determine whether the access is unauthorized based on such information. ● User Forensics: If an alarm event contains user behavior information, the user forensics information is displayed on the **Forensics** tab page. User forensics information includes the username, login IP address, login service type, login service port, last login event, and number of login failures. You can determine whether the access is unauthorized based on such information. ● **Registry Forensics**: If an alarm event contains registry information, you can check the registry keys and values on the **Forensics** tab page. You can locate registry risks based on such information. ● **Abnormal Login Forensics**: If an alarm event contains abnormal login information, you can check the login IP address and port number on the **Forensics** tab page. You can determine whether the login is trusted based on such information. ● **Malware Forensics**: If an alarm event contains malware information, you can check the malware family, virus name, virus type, and confidence level on the **Forensics** tab page. ● **Auto-started Item Forensics**: If an alarm event contains self-startup item information, you can check the malware family, virus name, virus type, and confidence level on the **Forensics** tab page. You can locate the auto-boot item based on the auto-started item forensics information. ● **Kernel Forensics**: If an alarm event contains kernel information, you can check system functions and kernel functions on the **Forensics** tab page. You can locate kernel risks based on the information.

Parameter	Description
Similar Alarms	Alarms that are similar to the current alarm event. You can handle the alarm according to the handling method of the similar alarms.

----End

6.1.1.3 Handling Server Alarms

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 urgent alarms, total alarms, servers with alarms, blocked IP addresses, and isolated files.

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

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

NOTE

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

Limitations and Constraints

- To skip the checks on high-risk command execution, privilege escalations, 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 **Viewing a Policy Group**.
- Other detection items cannot be manually disabled.
- Servers that are not protected by HSS do not support operations related to alarms and events.

Handling Server Alarm Events

This section describes how you should handle alarms to enhance server security.

NOTE

Do not fully rely on alarm handling 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Detection** > **Alarms** and click **Server Alarms**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Table 6-4 Alarm statistics

Parameter	Description
Enterprise Project	Select an enterprise project and view alarm details by enterprise project.
Time range	You can select a fixed period or customize a time range to search for alarms. Only alarms generated within 30 days can be queried. The options are as follows: ● Last 24 hours ● Last 3 days ● Last 7 days ● Last 30 days
Urgent Alarms	Number of urgent alarms that need to be handled.
Total Alarms	Total number of alarms on your assets.
Affected Servers	Number of servers for which alarms are generated. When checking alarms generated in the last 24 hours, you can click the number of servers to go to the **Servers & Quota** page and check the corresponding servers.
Handled Alarms	Number of handled alarms.

Parameter	Description
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 name, attack source IP address, login type, blocking status, number of blocks, blocking start time, and the latest blocking time. 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** ● The agent of Linux 3.2.10 or later supports IPv6 interception. The agent of a version earlier than Linux 3.2.10 supports TCP Wrapper interception, but does not support IPv6 interception using IPTables. ● After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address. ● A maximum of 10,000 IP addresses can be blocked for each type of software. If your Linux server does not support ipset, a maximum of 50 IP addresses can be clocked for MySQL and vsftp. If your Linux server does not support ipset or hosts.deny, a maximum of 50 IP addresses can be blocked for SSH.
Isolated Files	HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** 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 name to view the alarm details and suggestions.

Step 5 Handle alarms.

NOTE

Alarms are displayed on the **Server Alarms** page. Here you can check up to 30 days of historical alarms.

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

- Handling a single alarm

  In the **Operation** column of an alarm, click **Handle**.

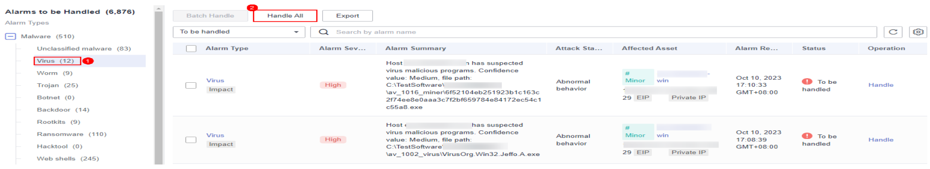
- Handling alarms in batches

  Select all alarms and click **Batch Handle** above the alarm list.

- Handling all alarms

  In the **Alarms to be Handled** area on the left pane of the alarm list, select an alarm type and click **Handle All** above the alarm list.

Figure 6-2 Handling all alarms



Alarms to be Handled (6,876)
Alarm Types
- Malware (510)
  - Unclassified malware (83)
  - Virus (12) 1
  - Worm (9)
  - Trojan (25)
  - Botnet (0)
  - Backdoor (14)
  - Rootkits (9)
  - Ransomware (110)
  - Hacktool (0)
  - Web shells (245)

	Alarm Type	Alarm Sev...	Alarm Summary	Attack Sta...	Affected Asset	Alarm Re...	Status	Operation
□	Virus Impact	High	Host [redacted] has suspected virus malicious programs. Confidence value: Medium, file path: C:\TestSoftware\ [redacted] \av_1016_miner\6f52104eb251923b1c163c2f74ee8e0aaa3c7f2bf659784e84172ec54c1c55a8.exe	Abnormal behavior	# Minor win [redacted] 29 EIP Private IP	Oct 10, 2023 17:10:33 GMT+08:00	To be handled	Handle
□	Virus Impact	High	Host [redacted] has suspected virus malicious programs. Confidence value: Medium, file path: C:\TestSoftware [redacted] \av_1002_virus\VirusOrg.Win32.Jeffo.A.exe	Abnormal behavior	# Minor win [redacted] 29 EIP Private IP	Oct 10, 2023 17:08:39 GMT+08:00	To be handled	Handle

Step 6 In the **Handle Event** dialog box, select an action. For details about the alarm handling actions, see **Table 6-5**.

When handling a single alarm event or handling alarms in batches, you can select **Handle duplicate alarms in batches** in the **Handle Event** dialog box.

Table 6-5 Alarm handling methods

Action	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**. For details about events that can be isolated and killed, see **Server Alarms**. **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.
Add to process whitelist	If you can confirm that a process triggering an alarm can be trusted, you can add it to the process whitelist. HSS will no longer report alarms on whitelisted processes.
Add to Login 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 Login Whitelist. A whitelisted login event will not trigger alarms. The following alarm events can be added: ● Brute-force attacks ● Abnormal logins

Action	Description
Add to alarm whitelist	Add false alarmed items to the login whitelist. HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms. After adding an alarm to the alarm whitelist, you can customize a whitelist rule. The custom rule types vary depending on the alarm types, including the file path, process path, process command line, remote IP address, and user name. If a detected alarm event hit the rule you specified, HSS does not generate an alarm. For details about events that can be isolated and killed, see **Server Alarms**.

Step 7 Click **OK**.

You check handled alarms. For details, see **Viewing the Handling History**.

----End

Canceling Handled Server Alarms

You can cancel the processing of a handled alarm event.

Step 1 In the alarm event list, filter handled alarms.

Step 2 In the **Operation** column of an alarm, click **Handle**.

Step 3 In the **Handle Alarm Event** dialog box, click **OK** to cancel the last handling.

----End

6.1.1.4 Exporting Server Alarms

You can export server alarms and events to a local PC.

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** > **HSS**.

Step 3 In the navigation pane, choose **Detection** > **Alarms**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Server Alarms** tab.

Step 5 Click **Export** above the alarm list to export all security events.

To export the alarms of a certain type or ATT&CK attack phase, select the type or phase in the **Alarms to Be Handled** area and click **Export**.

Step 6 View the export status in the upper part of the alarms page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

6.1.1.5 Managing Isolated Files

HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** page. You can click **Isolated Files** on the upper right corner to check them, and can recover or delete isolated files anytime.

For details about events that can be isolated and killed, see **Server Alarms**.

Constraints

Servers that are not protected by HSS do not support alarm-related operations.

Isolation and Killing Operations

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Detection** > **Alarms** and click **Server Alarms**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Table 6-6 Alarm statistics

Parameter	Description
Enterprise Project	Select an enterprise project and view alarm details by enterprise project.

Parameter	Description
Time range	You can select a fixed period or customize a time range to search for alarms. Only alarms generated within 30 days can be queried. The options are as follows: ● Last 24 hours ● Last 3 days ● Last 7 days ● Last 30 days
Urgent Alarms	Number of urgent alarms that need to be handled.
Total Alarms	Total number of alarms on your assets.
Affected Servers	Number of servers for which alarms are generated. When checking alarms generated in the last 24 hours, you can click the number of servers to go to the **Servers & Quota** page and check the corresponding servers.
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 name, attack source IP address, login type, blocking status, number of blocks, blocking start time, and the latest blocking time. 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** ● The agent of Linux 3.2.10 or later supports IPv6 interception. The agent of a version earlier than Linux 3.2.10 supports TCP Wrapper interception, but does not support IPv6 interception using IPTables. ● After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address. ● A maximum of 10,000 IP addresses can be blocked for each type of software. If your Linux server does not support ipset, a maximum of 50 IP addresses can be clocked for MySQL and vsftp. If your Linux server does not support ipset or hosts.deny, a maximum of 50 IP addresses can be blocked for SSH.

Parameter	Description
Isolated Files	HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** 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 Locate an event that can be isolated and killed, click **Handle** in the **Operation** column, and select **Isolate and Kill** in the displayed box.

NOTE

For details about events that can be isolated and killed, see **Server Alarms**.

Step 5 Click **OK** and isolate and kill the target alarm event.

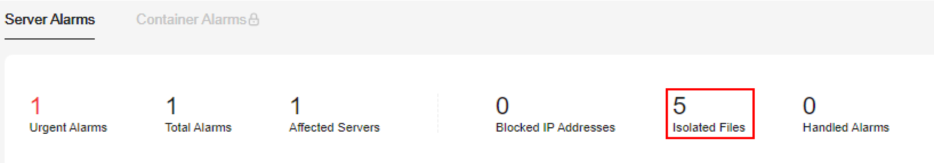
Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** page and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check them.

----End

Checking Isolated Files

Step 1 In the alarm statistics area on the **Server Alarms** page, click the number above **Isolated Files** to check the isolated files.

Figure 6-3 Alarm statistics



Step 2 Check the servers, names, paths, and modification time of the isolated files.

----End

Restoring Isolated Files

If you want to de-isolate an isolated file, you can restore it by referring to the following steps.

Step 1 Click restore in the **Operation** column of the file isolation box list. The restore isolated files dialog box is displayed.

Step 2 Click **OK**.

NOTE

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

----End

Deleting Isolated Files

If you want to permanently delete an isolated file, you can perform the deletion operation by referring to the following steps.

Step 1 Click **Delete** in the **Operation** column of the list. The dialog box is displayed.

To delete isolated files in batches, select multiple isolated files and click **Delete** in the upper left corner of the list.

Step 2 Click **OK**.

NOTE

Deleted isolated files cannot be restored. Exercise caution when performing this operation.

----End

6.1.2 Container Alarms

6.1.2.1 Container Alarm Events

After node protection is enabled, an agent is deployed on each container host to monitor the running status of containers in real time. The agents support escape detection, high-risk system calls, abnormal processes, abnormal files, and container environment detection. You can learn alarm events comprehensively on the **Container Alarms** page, and eliminate security risks in your assets in a timely manner.

Constraints

- Only HSS container edition supports the container security alarm function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- The container security alarm function supports intrusion detection and alarm reporting for the following Linux container runtime components:
  - Containerd
  - Docker

Container Alarm Types

Event Type	Alarm Name	Mechanism
Malware	Unclassified malware	Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing.

Event Type	Alarm Name	Mechanism
	Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.
	Web shells	Check whether the files (often PHP and JSP files) in the web directories on containers are web shells.
	Hacker tools	Report alarms on the malicious behaviors that exploit vulnerabilities or are performed using hacker tools.
Vulnerability Exploits	Vulnerability escapes	HSS reports an alarm if it detects container process behavior that matches the behavior of known vulnerabilities (such as Dirty COW, brute-force attack, runC, and shocker).
	File escapes	HSS reports an alarm if it detects that a container process accesses a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms.
Abnormal System Behaviors	Reverse shells	Monitor user process behaviors in real time to report alarms on and block 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 and automatic blocking in the **Malicious File Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands. You can also configure automatic blocking of reverse shells in the **HIPS Detection** rule on the **Policies** page.
	File privilege escalation	Report alarms on root privilege escalations exploiting SUID and SGID program vulnerabilities.

Event Type	Alarm Name	Mechanism
	Process privilege escalations	After hackers intrude containers, 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 can detect the following abnormal privilege escalation operations: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities ● File privilege escalation
	Important file changes	Monitor important system files (such as ls, ps, login, and top) in real time and generate alarms if these files are modified. For more information, see **Monitored important file paths**. HSS reports all the changes on important files, regardless of whether the changes are performed manually or by processes.
	Abnormal process behaviors	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
	High-risk system calls	CGS reports an alarm if it detects a high-risk call, such as **open_by_handle_at**, **ptrace**, **setns**, and **reboot**.
	High-risk command executions	Check executed commands in containers and generate alarms if high-risk commands are detected.

Event Type	Alarm Name	Mechanism
	Abnormal container processes	- Malicious container program HSS monitors container process behavior and process file fingerprints. It reports an alarm if it detects a process whose behavior characteristics match those of a predefined malicious program. - Abnormal processes If you are sure that only specific processes run in a container, you can whitelist the processes on the **Policy Groups** page, and associate the policy with the container. HSS reports an alarm if it detects that a process not in the whitelist is running in the container.
	Sensitive file access	HSS monitors the container image files associated with file protection policies, and reports an alarm if the files are modified.

Event Type	Alarm Name	Mechanism
	Abnormal container startups	HSS monitors container startups and reports an alarm if it detects that a container with too many permissions is started. This alarm does not indicate an actual attack. Attacks exploiting this risk will trigger other HSS container alarms. HSS container check items include: ● Privileged container startup (**privileged:true**) Alarms are triggered by the containers started with the maximum permissions. Settings that can trigger such alarms include the **–privileged=true** parameter in the **docker run** command, and **privileged: true** in the **securityContext** of the container in a Kubernetes pod. If the alarm name is **Container Security Options** and the alarm content contains **privileged:true**, it indicates that the container is started in privileged container mode. ● Too many container capabilities (**capability:[xxx]**) In Linux OSs, system permissions are divided into groups before assigned to containers. A container only has a limited number of permissions, and the impact scope of this container is limited in the case of an incident. However, malicious users can grant all the system permissions to a container by modifying its startup configurations. If the alarm name is **Container Security Options** and the alarm content contains **capabilities:[xxx]**, it indicates that the container is started with an overlarge capability set, which poses risks. ● Seccomp not enabled (**seccomp=unconfined**) Secure computing mode (seccomp) is a Linux kernel feature. It can restrict system calls invoked by processes to reduce the attack surface of the kernel. If **seccomp=unconfined** is configured when a container is started, system calls will not be restricted for the container. If the alarm name is **Container Security Options** and the alarm content contains **seccomp=unconfined**, it indicates that the container is started without seccomp, which poses risks. **NOTE** If seccomp is enabled, permissions will be verified for every system call. The verifications will probably affect services if system calls are frequent. Before you decide whether to enable seccomp, you are advised to test-enable it and analyze the impact on your services. ● Container privilege escalation (**no-new-privileges:false**)

Event Type	Alarm Name	Mechanism
		CGS reports an alarm if it detects that a process attempts to escalate permissions by running the **sudo** command and using the SUID or SGID bit. If **–no-new-privileges=false** is specified when a container is started, the container can escalate privileges. If the alarm name is **Container Security Options** and the alarm content contains **no-new-privileges:false**, it indicates that privilege escalation restriction is disabled for the container, which poses risks. ● High-risk directory mapping (**mounts:[...]**) For convenience purposes, when a container is started on a server, the directories of the server can be mapped to the container. In this way, services in the container can directly read and write resources on the server. However, this mapping incurs security risks. If any critical directory in the server OS is mapped to the container, improper operations in the container will probably damage the server OS. HSS reports an alarm if it detects that a critical server path (**/boot**, **/dev**, **/etc**, **/sys**, and **/var/run**) is mounted during container startup. If the alarm name is **Container Mount Point** and the alarm content contains **mounts: [{"source":"xxx","destination":"yyy"...]**, it indicates that a file path mapped to the container is unsafe. In this case, check for risky directory mappings. You can configure the mount paths that are considered secure in the container information collection policy. **NOTE** Alarms will not be triggered for the files that need to be frequently accessed by Docker containers, such as **/etc/hosts** and **/etc/resolv.conf**. ● Startup of containers in the **host** namespace The namespace of a container must be isolated from that of a server. If a container and a server use the same namespace, the container can access and modify the content on the server, which incurs container escape risks. To prevent such problems, HSS checks the container PID, network, and whether the container namespace is **host**. If the alarm name is **Container Namespace** and the alarm content contains **Container PID Namespace Mode**, **Container IPC Namespace Mode**, or **Container Network Namespace Mode**, it indicates that a container whose namespace is **host** is started. In this case, check the container startup options based

Event Type	Alarm Name	Mechanism
		on the alarm information. If you are sure that the container can be trusted, you can ignore the alarm.
	Container Image blocking	If a container contains insecure images specified in the **Suspicious Image Behaviors**, before the container is started, an alarm will be generated for the insecure images. **NOTE** You need to **install the Docker plug-in**.
	Suspicious command executions	● Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. ● Detect suspicious remote command execution.
Abnormal User Behaviors	Invalid accounts	Hackers can probably crack unsafe accounts on your containers and control the containers. HSS checks for suspicious hidden accounts and cloned accounts and generates alarms on them.
	Brute-force attacks	Detect and report alarms for brute-force attack behaviors, such as brute-force attack attempts and successful brute-force attacks, on containers. Detect SSH, web, and Enumdb brute-force attacks on containers. **NOTE** Currently, brute-force attacks can be detected only in the Docker runtime.
	Password thefts	Report alarms on user key theft.
Abnormal Network Access	Abnormal outbound connections	Report alarms on suspicious IP addresses that initiate outbound connections.
	Port forwarding	Report alarms on port forwarding using suspicious tools.
Abnormal Cluster Behaviors	Abnormal pod behaviors	Detect abnormal operations such as creating privileged pods, static pods, and sensitive pods in a cluster and abnormal operations performed on existing pods and report alarms.
	User information enumerations	Detect the operations of enumerating the permissions and executable operation list of cluster users and report alarms.

Event Type	Alarm Name	Mechanism
	Binding cluster roles	Detect operations such as binding or creating a high-privilege cluster role or service account and report alarms.
	Kubernetes event deletions	Detect the deletion of Kubernetes events and report alarms.

Monitored important file paths

Type	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

6.1.2.2 Viewing Container Alarms

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 urgent alarms, total alarms, containers with alarms, and handled alarms.

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

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

Constraints

Servers that are not protected by HSS do not support operations related to alarms and events.

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** > **HSS**.

Step 3 In the navigation pane, choose **Detection** > **Alarms** and click the **Container Alarms** tab to view container alarms and events.

- View the overview of container alarms and events.
  - **Urgent Alarms**: Number of urgent alarms that need to be handled. You can click the number to view the alarm list.
  - **Total Alarms**: Total number of alarms reported on your assets. You can click the number to view all alarms.
  - **Containers with Alarms**: Number of containers with alarms.
  - **Handled Alarms**: Number of handled alarms.
- View the alarms of a certain type or ATT&CK phase.

  In the **Alarms to Be Handled** area, select an alarm type or att&ck phase.

  ATT&CK attack phase tags are also displayed below alarm names. For more information, see **Table 6-7**.

  NOTE

  Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a framework that helps organizations understand the cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle.

Table 6-7 ATT&CK phases

ATT&CK Phase	Description
Reconnaissance	Attackers seek vulnerabilities in your system or network.
Initial Access	Attacker try to enter your system or network.
Execution	Attackers try to run malicious code.
Persistence	Attackers try to maintain their foothold.
Privilege Escalation	Attackers try to obtain higher permissions.
Defense Evasion	Attackers try to avoid being detected.
Credential Access	Attackers try to steal account names and passwords.
Command and Control	Attackers try to communicate with compromised machines to control them.
Impact	Attackers try to manipulate, interrupt, or destroy your system or data.

- View details about container alarms and events.

Click an alarm name to go to its details page. You can view the alarm description, handling suggestion, alarm path and address in HSS forensics, and the handling history of similar alarms. **Table 6-8** describes the details of alarm information.

NOTE

You can download the alarm source files of certain malware to your local PC for analysis. The password for decompressing the files is **unlock**.

Table 6-8 Alarm detail parameters

Parameter	Description
Intelligence Engine	Detection engines used by HSS, including the virus detection engine, AI detection engine, and malicious intelligence detection engine.
Attack Status	Status of the current threat.
First Occurred	Time when an attack alarm is generated for the first time
Alarm ID	Unique ID of an alarm
ATT&CK Phase	For details about the attack technology models used by attackers in each phase, see **Table 6-7**.
Last Occurred	Time when an attack alarm is generated for the last time
Alarm Information	Detailed information about an alarm, including the alarm description, alarm summary, affected assets, and handling suggestions.

Parameter	Description
Forensics	HSS investigates information such as the attack triggering path or virus type based on the alarm type, helping you quickly trace and locate the attack source. – **Process Tree**: If an alarm event contains process information, you can check the process ID, process file path, process command line, process startup time, and process file hash on the **Forensics** tab page. You can locate malicious processes based on such information. – **File Forensics**: If an alarm event contains file information, you can check the file path and file hash on the **Forensics** tab page. You can locate the file change based on the such information. – Network Forensics: If an alarm event contains network-related information, you can check the local IP address, local port, remote IP address, remote port, and protocol on the **Forensics** tab. You can determine whether a user is unauthorized based on such information. – User Forensics: If an alarm event contains user-related information, you can check the user name, login IP address, login service type, login service port, last login event, and number of login failures on the **Forensics** tab. You can determine whether the access is unauthorized based on such information. – **Registry Forensics**: If an alarm event contains registry information, you can check the registry keys and values on the **Forensics** tab page. You can locate registry risks based on such information. – **Abnormal Login Forensics**: If an alarm event contains abnormal login information, you can check the login IP address and port number on the **Forensics** tab page. You can determine whether the login is trusted based on such information. – **Malware Forensics**: If an alarm event contains malware information, you can check the malware family, virus name, virus type, and confidence level on the **Forensics** tab page. – Self-startup item evidence collection information: If an alarm event contains self-startup item information, the self-startup item evidence collection information is displayed in the investigation and evidence collection column. You can locate the auto-boot items based on such information. – **Kernel Forensics**: If an alarm event contains kernel information, you can check system functions and kernel functions on the **Forensics** tab page. You can locate kernel risks based on the information. – **Container Forensics**: If an alarm event contains container information, you can check the container name and image

Parameter	Description
	ID on the **Forensics** tab page. You can locate container risks based on such information.
Similar Alarms	Alarms that are similar to the current alarm event. You can handle the alarm according to the handling method of the similar alarms.

- View the pod details of the container alarm event.

  Click the pod name of the target alarm event to view the pod details, including the node IP address, namespace, pod IP address, pod label, and container list.

----End

6.1.2.3 Handling Container Alarms

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 urgent alarms, total alarms, containers with alarms, and handled alarms.

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

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

Constraints

Servers that are not protected by HSS do not support operations related to alarms and events.

Handling Container Alarm Events

This section describes how you should handle alarms to enhance server security.

NOTE

Do not fully rely on alarm handling 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Detection** > **Alarms**, and click **Container Alarms**.

Table 6-9 Alarm statistics

Alarm Event	Description
Urgent Alarms	Number of urgent alarms that need to be handled.
Total Alarms	Total number of alarms on your assets.
Containers with Alarms	Number of containers for which alarms are generated.
Handled Alarms	Number of handled alarms.

Step 4 Click an alarm name to view the alarm details and suggestions.

Step 5 Handle alarms.

NOTE

Alarms are displayed on the **Container Alarms** page. Here you can check up to 30 days of historical alarms.

Check and handle alarms as needed. The status of a handled alarm changes from **Unhandled** to **Handled**. HSS will no longer collect its statistics.

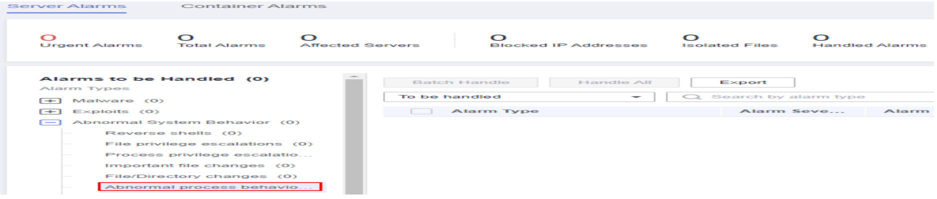
- Handling a single alarm

  In the **Operation** column of an alarm, click **Handle**.
- Handling alarms in batches

  Select all alarms and click **Batch Handle** above the alarm list.
- Handling all alarms

  In the **Alarms to be Handled** area on the left pane of the alarm list, select an alarm type and click **Handle All** above the alarm list.

Figure 6-4 Handling all alarms



Step 6 In the **Handle Event** dialog box, select an action. For details about the processing modes, see **Table 6-10**.

When handling a single alarm event or handling alarms in batches, you can select **Handle duplicate alarms in batches** in the **Handle Event** dialog box.

Table 6-10 Alarm handling methods

Action	Description
Ignore	Ignore the current alarm. Any new alarms of the same type will still be reported by HSS.

Action	Description
Mark as handled	Mark the event as handled. You can add remarks for the event to record more details.
Add to Login 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 Login Whitelist. A whitelisted login event will not trigger alarms. If the login IP address has been blocked, adding the login alarm event to the Login Whitelist will unblock the login IP address. The following alarm events can be added: ● Brute-force attacks ● Abnormal logins
Add to process whitelist	If you can confirm that a process triggering an alarm can be trusted, you can add it to the process whitelist.
Add to alarm whitelist	Add false alarmed items to the login whitelist. HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms. After adding an alarm to the alarm whitelist, you can customize a whitelist rule. The custom rule types vary depending on the alarm types, including the file path, process path, process command line, remote IP address, and user name. If a detected alarm event hit the rule you specified, HSS does not generate an alarm. For details about events that can be isolated and killed, see **Container Alarm Events**.

Step 7 Click **OK**.

You check handled alarms. For details, see **Historical Records**.

----End

Canceling Handled Container Alarms

You can cancel the processing of a handled alarm event.

Step 1 In the alarm event list, filter handled alarms.

Step 2 In the **Operation** column of an alarm, click **Handle**.

Step 3 In the **Handle Alarm Event** dialog box, click **OK** to cancel the last handling.

----End

6.1.2.4 Exporting Container Alarms

You can export container alarms and events to a local PC.

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** > **HSS**.

Step 3 In the navigation pane, choose **Detection** > **Alarms**.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click the **Container Alarms** tab.

Step 5 Click **Export** above the alarm list to export all security events.

To export the alarms of a certain type or ATT&CK attack phase, select the type or phase in the **Alarms to Be Handled** area and click **to export**.

Step 6 View the export status in the upper part of the alarms page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

6.2 Whitelist Management

6.2.1 Managing Login Whitelist

You can configure the IP addresses of destination servers, login IP addresses, login usernames, and user behaviors in the Login Whitelist.

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 Whitelist**, the alarms (if any) that have been generated for the IP address will not be automatically cleared. Handle the alarms by referring to **Viewing Server Alarms**.
- To unblock IP addresses, add the IP address to the whitelist of the login security detection policy. For details, see **Login Security Check**.

You can add Login Whitelist in either of the following ways:

- Add it to the Login Whitelist when handling false alarms of the **Brute-force attack** and **Abnormal login** types. For details, see **Viewing Server Alarms**.

- On the Login Whitelist page, add Login Whitelist.

Adding Login Whitelist

Step 1 Log in to the management console.

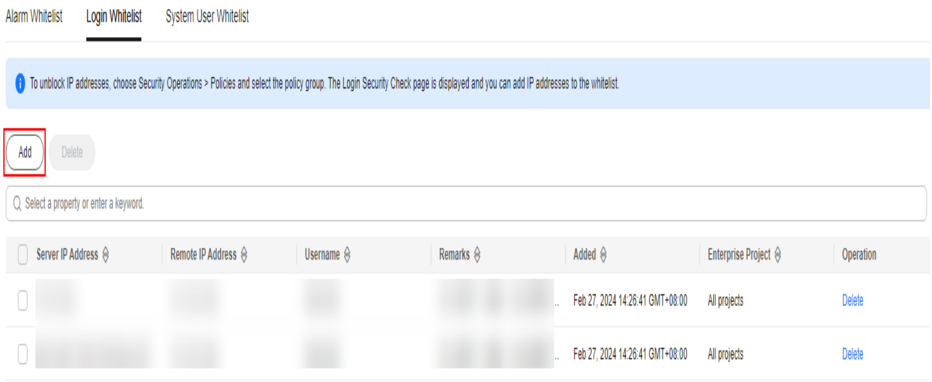
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Detection** > **Whitelists** > **Login Whitelist** to access the **Whitelists** page, and click **Add**.

📖 NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 6-5 Adding Login Whitelist



Alarm Whitelist | Login Whitelist | System User Whitelist

To unblock IP addresses, choose Security Operations > Policies and select the policy group. The Login Security Check page is displayed and you can add IP addresses to the whitelist.

Add | Delete

Select a property or enter a keyword.

Server IP Address	Remote IP Address	Username	Remarks	Added	Enterprise Project	Operation
[redacted]	[redacted]	[redacted]	[redacted]	Feb 27, 2024 14:26:41 GMT+08:00	All projects	Delete
[redacted]	[redacted]	[redacted]	[redacted]	Feb 27, 2024 14:26:41 GMT+08:00	All projects	Delete

Step 4 On the displayed page, enter the server IP address, login IP address, and login username.

Table 6-11 Login security whitelist parameters

Parameter	Description	Example Value
Server IP Address	- IPv4 addresses are supported - Single IP addresses, IP address segments, and masks are supported. Use commas (,) to separate them.	- 192.168.1.1 - 192.168.2.1-192.168.6.1 - 192.168.7.0/24
Login IP Address		
Login Username	Current login username	hss_test
Remarks	Custom whitelist description	Test

Step 5 Click **OK**.

----End

Other Operations

Removing Login Whitelist

To delete a Login Whitelist, select the Login Whitelist to you want to delete and click **Delete**, or click **Delete** in the **Operation** column of the server IP address you want to delete in the Login Whitelist.

NOTE

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

6.2.2 Managing the Alarm Whitelist

You can configure the alarm whitelist to reduce false alarms. Events can be deleted from the whitelist.

Whitelisted events will not trigger alarms.

On the **Alarms** page, you can add falsely reported alarms to the alarm whitelist. After an alarm is added to the whitelist, HSS will not generate alarms or collect statistics on it.

Adding Events to the Alarm Whitelist

Table 6-12 Configuring the alarm whitelist

Method	Description
Add to alarm whitelist	Choose to add the alarm to the whitelist when handling it. The following types of events can be added to the alarm whitelist: ● Reverse shells ● Ransomware ● Malicious programs ● Web shell ● Abnormal process behaviors ● Process privilege escalations ● File privilege escalations ● High-risk command executions ● Malicious programs ● Important file changes ● File/Directory changes ● Abnormal shells ● Suspicious crontab tasks ● Invalid accounts ● Common vulnerability exploits ● Redis vulnerability exploits ● Hadoop vulnerability exploits ● MySQL vulnerability exploits

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** > **HSS**.

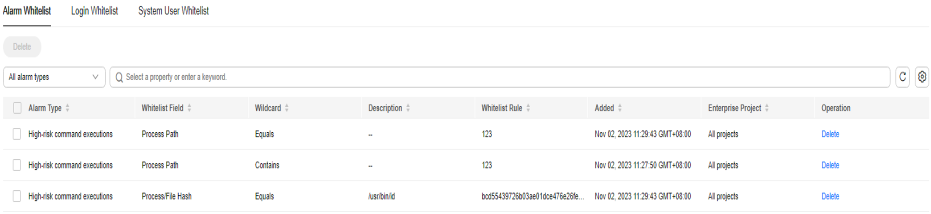
Step 3 In the navigation pane on the left, choose **Detection** > **Whitelists**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click **Alarm Whitelist** to view the added alarm whitelist. For more information, see **Table 6-13**.

Figure 6-6 Alarm whitelist



Alarm Type	Whitelist Field	Wildcard	Description	Whitelist Rule	Added	Enterprise Project	Operation
High-risk command executions	Process Path	Equals	--	123	Nov 02, 2023 11:29:43 GMT+08:00	All projects	Delete
High-risk command executions	Process Path	Contains	--	123	Nov 02, 2023 11:27:50 GMT+08:00	All projects	Delete
High-risk command executions	Process/File Hash	Equals	/usr/bin/id	bcd55439726b03ae01dce476e26fe...	Nov 02, 2023 11:29:43 GMT+08:00	All projects	Delete

Table 6-13 Parameter description

Parameter Name	Description
Alarm Type	Name of the alarm whitelist type.
Whitelist Field	Whitelisted file field
Wildcard	Logic used by a whitelisted rule, which can be equal or include.
Whitelist Rule	Whitelisted rule ID
Description	Description of the target whitelist.
Data Source	Source of the target whitelist.
Added	Time when an alarm is added to the whitelist.
Enterprise Project	Enterprise project

----End

Related Operations

Removing alarms from the whitelist

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

NOTE

- Exercise caution when performing this operation. Whitelisted alarms cannot be restored after removal, and will be reported once triggered.
- After an alarm is deleted from the whitelist, the handling status of the events associated with the alarm is not updated. To change the status, choose **Detection** > **Alarms**, click **Handle** in the **Operation** column of an event, and select **Remove from whitelist**.

6.2.3 Managing the System User Whitelist

HSS generates risky account alarms when non-root users are added to the root user group. You can add the trusted non-root users to the system user whitelist. HSS does not generate risky account alarms for users in the system user whitelist.

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** > **HSS**.

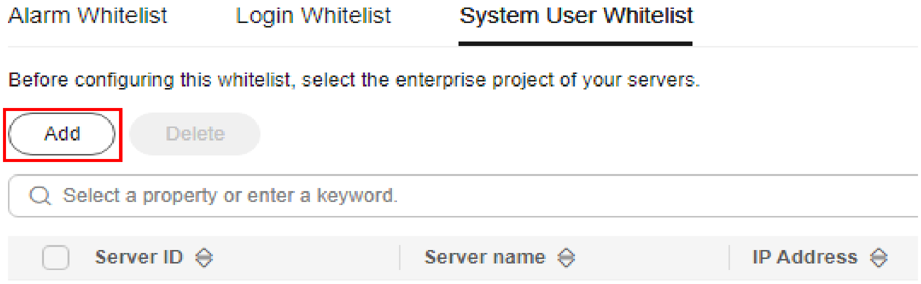
Step 3 In the navigation pane on the left, choose **Detection** > **Whitelists**. The **Whitelists** page is displayed.

Step 4 (Optional) In the upper left corner of the **Whitelists** page, select the enterprise project to which the server belongs or **All projects** for **Enterprise Project**.

If you have not enabled the enterprise project function, skip this step.

Step 5 Click the **System User Whitelist** tab and click **Add**.

Figure 6-7 Configuring the system user whitelist



Before configuring this whitelist, select the enterprise project of your servers.

Step 6 In the **Add to System User Whitelist** dialog box, enter the server ID, system username, and remarks.

Step 7 Click **OK**.

----End

Related Operations

Modifying a System User Whitelist

Step 1 (Optional) In the upper left corner of the **Whitelists** page, select the enterprise project to which the server belongs or **All projects** for **Enterprise Project**.

If you have not enabled the enterprise project function, skip this step.

Step 2 In the row of the target system user whitelist, click **Modify** in the **Operation** column.

Step 3 In the **Modify System User Whitelist** dialog box, modify the information and click **OK**.

----End

Deleting a System User Whitelist

Step 1 (Optional) In the upper left corner of the **Whitelists** page, select the enterprise project to which the server belongs or **All projects** for **Enterprise Project**.

If you have not enabled the enterprise project function, skip this step.

Step 2 In the row of the target system user whitelist, click **Delete** in the **Operation** column.

You can also select multiple system user whitelists and click **Delete** in the upper left corner of the system user whitelist list.

Step 3 In the dialog box displayed, click **OK**.

----End

7 Security Operations

7.1 Policy Management

7.1.1 Overview

If policies such as asset collection, baseline check, and intrusion detection do not meet your server protection requirements, you can manage these policies.

Table 7-1 lists the policies that can be managed by each HSS edition. For details about how to configure policies, see **Configuring Policies**.

If you have different protection requirements, you can create a custom policy group to deploy different protection policies for different servers. For details, see **Creating a Policy Group**.

Table 7-1 Policies

Function Type	Policy	Action	Supported OS	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Assets	Asset discovery	Scan and display all software in one place, including software name, path, and major applications, helping you identify abnormal assets.	Linux and Windows	×	×	√	√	√

Function Type	Policy	Action	Supported OS	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Baseline Inspection	Weak password detection	Change weak passwords to stronger ones based on HSS scan results and suggestions.	Linux	√	√	√	√	√
	Container information collection	Collect information about all containers on a server, including ports and directories, and report alarms for risky information.	Linux	×	×	×	×	√
	Configuration Check	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.	Linux and Windows	×	×	√	√	√

Function Type	Policy	Action	Supported OS	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Intrusions	AV detection	Check server assets and report, isolate, and kill the detected viruses. The generated alarms are displayed under **Detection** > **Alarms** > **Server Alarms** > **Event Types** > **Malware**. After AV detection is enabled, the resource usage is as follows: The CPU usage does not exceed 40% of a single vCPU. The actual CPU usage depends on the server status. For details, see **How Many CPU and Memory Resources Are Occupied by the Agent When It Performs Scans?**	Windows	√	√	√	√	×
	Cluster intrusion detection	Detect container high-privilege changes, creation in key information, and virus intrusion.	Linux	×	×	×	×	√
	Container escape	Check for and generate alarms on container escapes.	Linux	×	×	×	×	√

Function Type	Policy	Action	Supported OS	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Container information module	This function is used to mask intrusion detection alarms of trusted containers. You can configure a trusted container whitelist based on the container name, organization name to which the image belongs, and namespace so that intrusion detection does not detect these trusted containers.	Linux	×	×	×	×	√
	Web Shell Detection	Scan web directories on servers for web shells.	Linux and Windows	√	√	√	√	√
	Container File Monitoring	Detect file access that violates security policies. Security O&M personnel can check whether hackers are intruding and tampering with sensitive files.	Linux	×	×	×	×	√
	Container Process Whitelist	Check for process startups that violate security policies.	Linux	×	×	×	×	√
	Suspicious Image Behaviors	Configure the blacklist and whitelist and customize permissions to ignore abnormal behaviors or report alarms.	Linux	×	×	×	×	√

Function Type	Policy	Action	Supported OS	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	HIPS Detection	Check registries, files, and processes, and report alarms for operations such as abnormal changes.	Linux and Windows	×	√	√	√	√
	File Protection	Check the files in the Linux OS, applications, and other components to detect tampering.	Linux	√	√	√	√	√
	Login Security Check	Detect brute-force attacks on SSH, FTP, 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.	Linux and Windows	√	√	√	√	√

Function Type	Policy	Action	Supported OS	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Malicious File Detection	● Reverse shell: Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. ● Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	Linux	√	√	√	√	√
	Port Scan Detection	Detect scanning or sniffing on specified ports and report alarms.	Linux	×	×	√	√	√
	Abnormal process behaviors	All the running processes on all your servers are monitored for you. You can create a process whitelist to ignore alarms on trusted processes, and can receive alarms on unauthorized process behavior and intrusions.	Linux	√	√	√	√	√
	Root privilege escalation	Detect the root privilege escalation for files in the current system.	Linux	√	√	√	√	√

Function Type	Policy	Action	Supported OS	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Real-time process	Monitor the executed commands in real time and generate alarms if high-risk commands are detected.	Linux and Windows	√	√	√	√	√
	Rootkit Detection	Detect server assets and report alarms for suspicious kernel modules, files, and folders.	Linux	√	√	√	√	√

Function Type	Policy	Action	Supported OS	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Self-protection	Self-protection	Protect HSS files, processes, and software from malicious programs, which may uninstall HSS agents, tamper with HSS files, or stop HSS processes. ● Self-protection depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled. ● Enabling the self-protection policy has the following impacts: – The HSS agent cannot be uninstalled on the control panel of a server, but can be uninstalled on the HSS console. – HSS process cannot be terminated. – In the agent installation path **C:\Program Files \HostGuard**, you can only access the **log** and **data** directories (and the **upgrade**	Windows	×	×	√	√	×

Function Type	Policy	Action	Supported OS	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
		directory, if your agent has been upgraded).						

7.1.2 Creating a Policy Group

For premium and container editions, you can copy a policy group and customize it as required to meet server security requirements in different application scenarios.

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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Security Operation** > **Policies**. On the displayed page, **Policy group parameters** describes the fields.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Table 7-2 Policy group parameters

Parameter	Description
Policy Group	Name of a policy group The preset policy group names are as follows: ● **tenant_linux_advanced_default_policy_group**: preset policy of the Linux professional edition, which can only be viewed but cannot be copied or deleted. ● **tenant_windows_advanced_default_policy_group**: preset policy of the Windows professional edition, which can only be viewed but cannot be copied or deleted. ● **tenant_linux_container_default_policy_group**: preset Linux policy of the container edition. You can copy this policy group and create a new one based on it. ● **tenant_linux_enterprise_default_policy_group** is the default Linux policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. ● **tenant_windows_enterprise_default_policy_group**: preset Windows policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. ● **tenant_linux_premium_default_policy_group**: preset Linux policy of the premium edition. You can create a policy group by copying this default group and modify the copy. ● **tenant_windows_premium_default_policy_group**: preset Windows policy of the premium edition. You can create a policy group by copying this default group and modify the copy. ● **wtp_***ServerName* is a WTP edition policy group. It is generated by default when WTP is enabled for a server.
ID	Unique ID of a policy group
Description	Description of a policy group
Supported Version	HSS edition supported by a policy group.
Supported OS	OS supported by the policy.
Associated Servers	To view details about the servers associated with a policy group, click the number in the **Servers** column of the group.

Step 4 Select an enterprise or container edition policy group and click **Copy** in the **Operation** column of the policy group.

Step 5 In the dialog box displayed, enter a policy group name and description, and click **OK**.

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.

Step 6 Click **OK**.

After a policy group is created, you can configure rules for each policy in the policy group. For details, see **Configuring Policies**.

----End

Follow-up Procedure

After creating a policy group and configuring policies, you can apply the new policy group to servers. For details, see **Deploying a Protection Policy**.

7.1.3 Configuring Policies

After HSS is enabled, you can configure HSS policies based on your service requirements.

Constraints

- The professional, enterprise, premium, WTP, or container edition is enabled.
- For the default policy groups, you are advised to retain their default configurations.
- 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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Security Operation** > **Policies**. On the displayed page, **Policy group parameters** describes the fields.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Table 7-3 Policy group parameters

Parameter	Description
Policy Group	Name of a policy group The preset policy group names are as follows: ● **tenant_linux_advanced_default_policy_group**: preset policy of the Linux professional edition, which can only be viewed but cannot be copied or deleted. ● **tenant_windows_advanced_default_policy_group**: preset policy of the Windows professional edition, which can only be viewed but cannot be copied or deleted. ● **tenant_linux_container_default_policy_group**: preset Linux policy of the container edition. You can copy this policy group and create a new one based on it. ● **tenant_linux_enterprise_default_policy_group** is the default Linux policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. ● **tenant_windows_enterprise_default_policy_group**: preset Windows policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. ● **tenant_linux_premium_default_policy_group**: preset Linux policy of the premium edition. You can create a policy group by copying this default group and modify the copy. ● **tenant_windows_premium_default_policy_group**: preset Windows policy of the premium edition. You can create a policy group by copying this default group and modify the copy. ● **wtp_***ServerName* is a WTP edition policy group. It is generated by default when WTP is enabled for a server.
ID	Unique ID of a policy group
Description	Description of a policy group
Supported Version	HSS edition supported by a policy group.
Supported OS	OS supported by the policy.
Associated Servers	To view details about the servers associated with a policy group, click the number in the **Servers** column of the group.

Step 4 Click the name of the policy group to access the policy detail list.

NOTE

You can click **Enable** or **Disable** in the **Operation** column of a policy. After a policy is disabled, the detection of the policy is not performed.

Step 5 You can modify the policy by clicking its name.

----End

Asset Discovery

Step 1 Click **Asset Discovery**.

Step 2 On the displayed page, modify the settings as required. For more information, see **Table 7-4**.

Table 7-4 Parameter description

Parameter	Description
Scan Time	Fixed time for automatic assets scan. The scan time can be customized for middleware, web frameworks, kernel modules, web applications, websites, web services, and databases. Offset time is the automatic adjust ahead of or behind the specified scan time. ● Accounts: Linux accounts are automatically checked every hour, and Windows accounts are checked in real time. ● Open ports are automatically checked every 30 seconds. ● Processes are automatically checked every hour. ● Installed software is automatically checked once a day. ● Auto-startup items are automatically checked every hour. ● Middleware/Web framework: You can select the scan date and time together. ● Kernel modules: You can set the scan date and time as required. ● Web applications/Websites/Web services/Databases: You can select the scan date and time together.
Scanned Web Directories	Specifies a web directory to be scanned.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Weak Password Scan

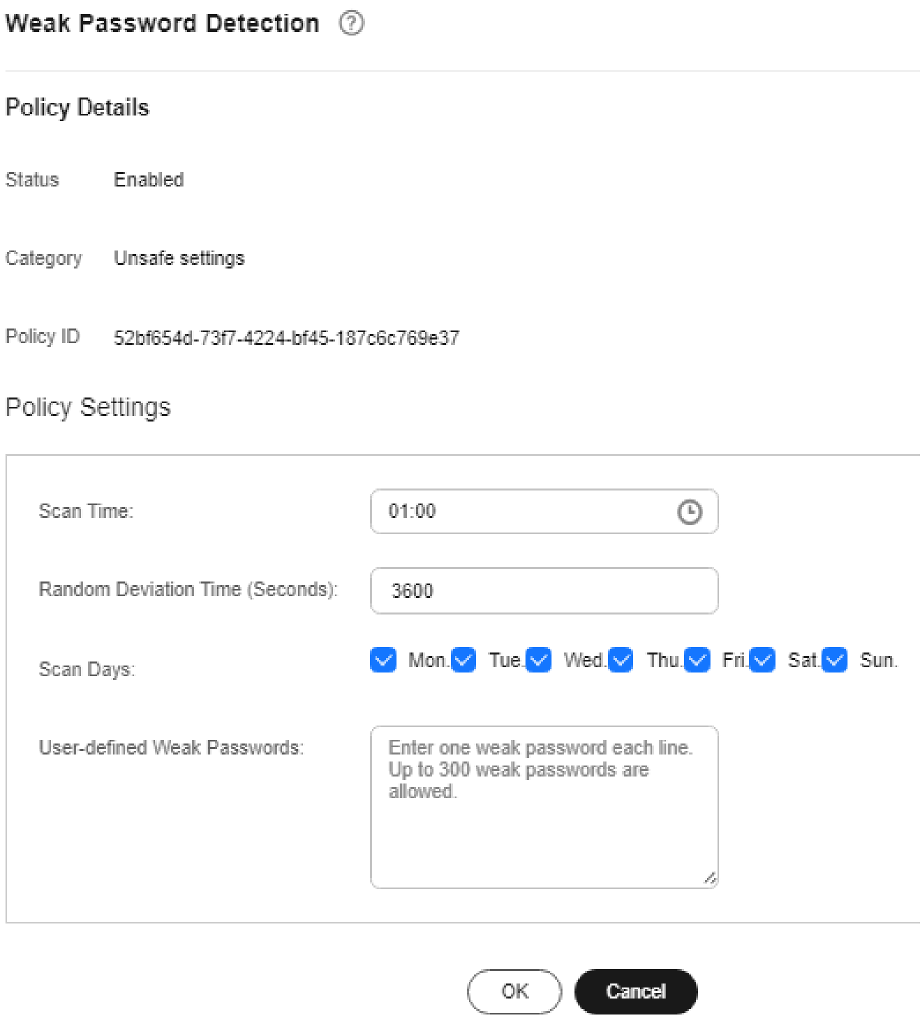
Weak passwords are not attributed to a certain type of vulnerabilities, but they bring no less security risks than any type of vulnerabilities. Data and programs will become insecure if their passwords are cracked.

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 Click **Weak Password Detection**.

Step 2 In the **Policy Settings** area, modify the settings as required. For more information, see **Table 7-5**.

Figure 7-1 Modifying the weak password detection policy



Weak Password Detection

Policy Details

Status Enabled

Category Unsafe settings

Policy ID 52bf654d-73f7-4224-bf45-187c6c769e37

Policy Settings

Scan Time: 01:00

Random Deviation Time (Seconds): 3600

Scan Days: ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. ☑ Sat. ☑ Sun.

User-defined Weak Passwords: Enter one weak password each line. Up to 300 weak passwords are allowed.

Table 7-5 Parameter description

Parameter	Description
Scan Time	Time point when detections are performed. It can be accurate to the minute.
Random Deviation Time (s)	Random deviation time of the weak password based on **Scan Time**. The value range is 0 to 7200s.
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. Enter only one weak password per line. Up to 300 weak passwords can be added.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

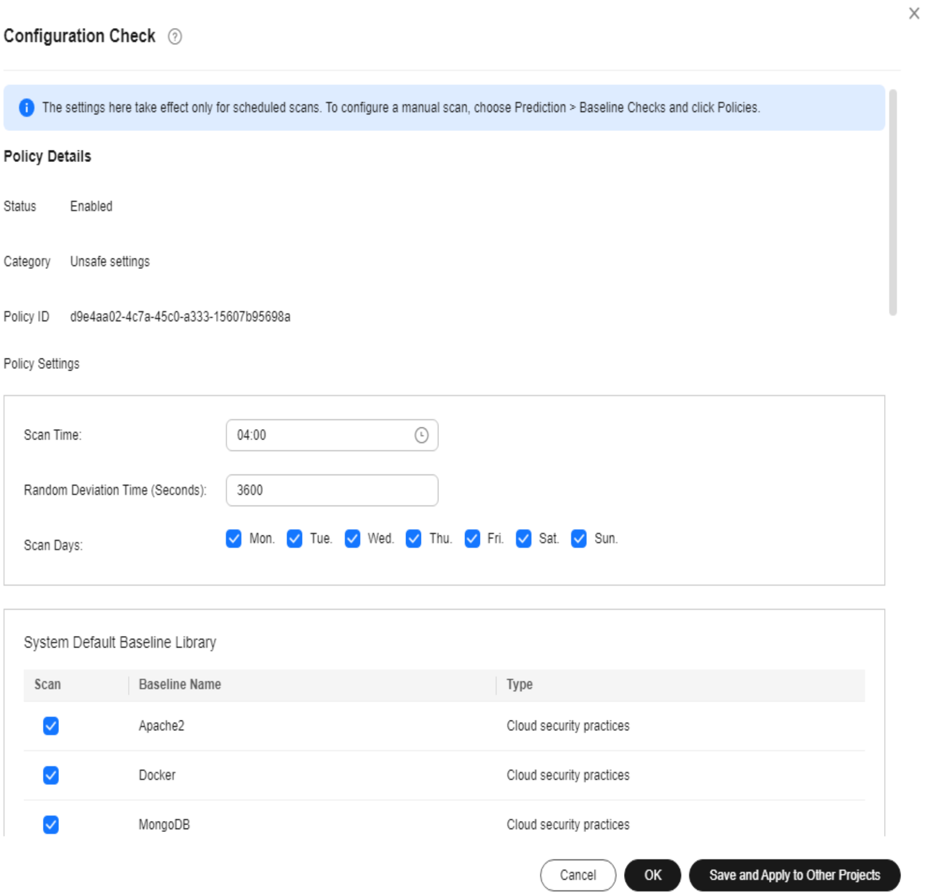
----End

Configuration Check

Step 1 Click **Configuration Check**.

Step 2 On the **Configure Check**, modify the policy.

Figure 7-2 Modifying the configuration check policy



Configuration Check

The settings here take effect only for scheduled scans. To configure a manual scan, choose Prediction > Baseline Checks and click Policies.

Policy Details

Status Enabled

Category Unsafe settings

Policy ID d9e4aa02-4c7a-45c0-a333-15607b95698a

Policy Settings

Scan Time: 04:00

Random Deviation Time (Seconds): 3600

Scan Days: ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. ☑ Sat. ☑ Sun.

System Default Baseline Library

Scan	Baseline Name	Type
☑	Apache2	Cloud security practices
☑	Docker	Cloud security practices
☑	MongoDB	Cloud security practices

Table 7-6 Parameter description

Parameter	Description
Scan Time	Time point when detections are performed. It can be accurate to the minute.
Random Deviation Time (Seconds)	Random deviation time of the system detection. The value ranges from 0 to 7,200s.
Scan Days	Day in a week when a detection is performed. You can select any days from Monday to Sunday.
System Default Baseline Library	The detection baseline has been configured in the system. You only need to select the baseline you want to scan. All parameters are in their default values and cannot be modified.

Step 3 Select the baseline to be detected or customize a baseline.

NOTE

To check whether your system meets compliance requirements, select **DJCP MLPS** in the **Type** area.

Step 4 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

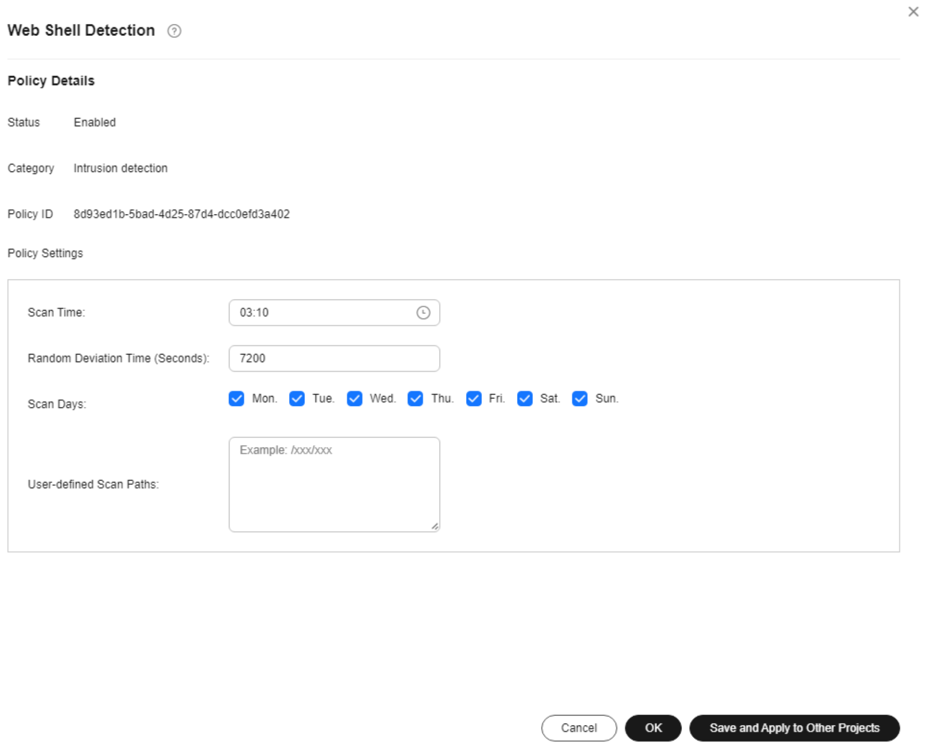
Web Shell Detection

If **User-defined Scan Paths** is not specified, the website paths in your assets are scanned by default. If **User-defined Scan Paths** is specified, only the specified paths are scanned.

Step 1 Click **Web Shell Detection**.

Step 2 On the **Web Shell Detection** page, modify the settings as required. For more information, see **Table 7-7**.

Figure 7-3 Modifying the web shell detection policy



Web Shell Detection

Policy Details

Status Enabled

Category Intrusion detection

Policy ID 8d93ed1b-5bad-4d25-87d4-dcc0efd3a402

Policy Settings

Scan Time: 03:10

Random Deviation Time (Seconds): 7200

Scan Days: ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. ☑ Sat. ☑ Sun.

User-defined Scan Paths: Example: /xxx/xxx

Table 7-7 Parameter description

Parameter	Description
Scan Time	Time point when detections are performed. It can be accurate to the minute.
Random Deviation Time (Seconds)	Random deviation time. The value ranges from 0 to 7,200s.

Parameter	Description
Scan Days	Days in a week when web shells are scanned. You can select one or more days.
User-defined Scan Paths	Web paths to be scanned. A file path must: ● Start with a slash (/) and end with no slashes (/). ● Occupy a separate line and cannot contain spaces.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

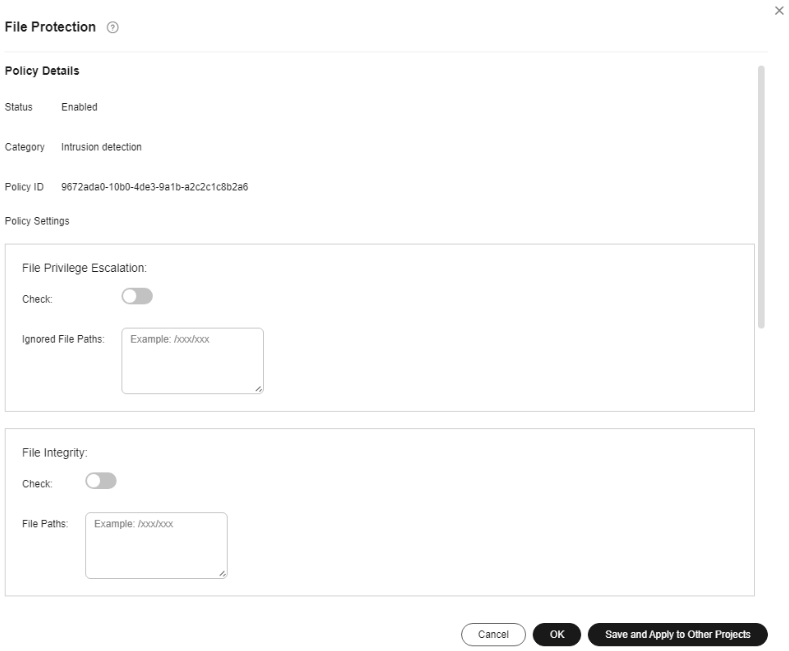
----End

File Protection

Step 1 Click **File Protection**.

Step 2 On the **File Protection** page, modify the policy. For more information, see **Table 7-8**.

Figure 7-4 File protection



File Protection

Policy Details

Status Enabled

Category Intrusion detection

Policy ID 9672ada0-10b0-4de3-9a1b-a2c2c1c8b2a6

Policy Settings

File Privilege Escalation:

Check: ○

Ignored File Paths: Example: /xxx/xxx

File Integrity:

Check: ○

File Paths: Example: /xxx/xxx

Table 7-8 Parameter description

Parameter	Description
File Privilege Escalation	● Enabled: Detects privilege escalation. – : enabled – : disabled ● **Ignored File Path**: Files to be ignored. Start the path with a slash (/) and do not end it with a slash (/). Each path occupies a line. No spaces are allowed between path names.
File Integrity	● Enabled: Detects the integrity of key files. – : enabled – : disabled ● **File Paths**: Configure the file paths.
Important File Directory Change	● Enabled: Detects the directory change of key files. – : enabled – : disabled ● **Session IP Whitelist**: If the file process belongs to the sessions of the listed IP addresses, no audit applies. ● **Unmonitored File Types**: File types that do not need to be monitored. ● **Unmonitored File Paths**: File paths that do not need to be monitored. ● **Monitoring Login Keys**: monitors login keys. – : enabled – : disabled
Directory Monitoring Mode	● Directory monitoring mode. ● **File or Directory Path**: Some file or directory monitoring paths are preset in the system. You can modify the file change type to be detected and add the file or directory paths to be monitored.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

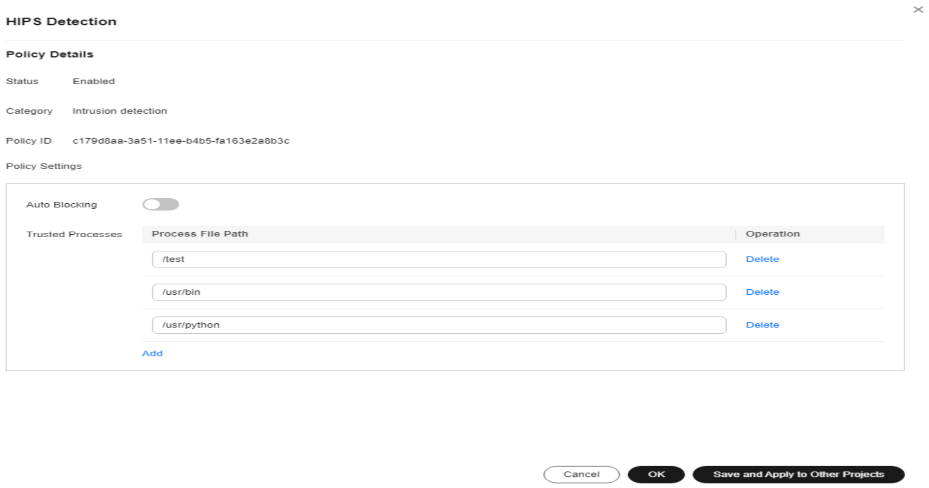
----End

HIPS Detection

Step 1 Click **HIPS Detection**.

Step 2 Modify the policy content. For more information, see **Table 7-9**.

Figure 7-5 Modifying the HIPS detection policy



HIPS Detection

Policy Details

Status Enabled

Category Intrusion detection

Policy ID c179d8aa-3a51-11ee-b4b5-fa163e2a8b3c

Policy Settings

Auto Blocking ○

Trusted Processes

Process File Path	Operation
/test	Delete
/usr/bin	Delete
/usr/python	Delete

Add

Table 7-9 HIPS detection policy parameters

Parameter	Description
Auto Blocking	If this function is enabled, abnormal changes on registries, files, and processes will be automatically blocked to prevent reverse shells and high-risk commands. - ●: enabled - ○: disabled
Trusted Processes	Paths of trusted processes. You can click **Add** to add a path and click **Delete** to delete it.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

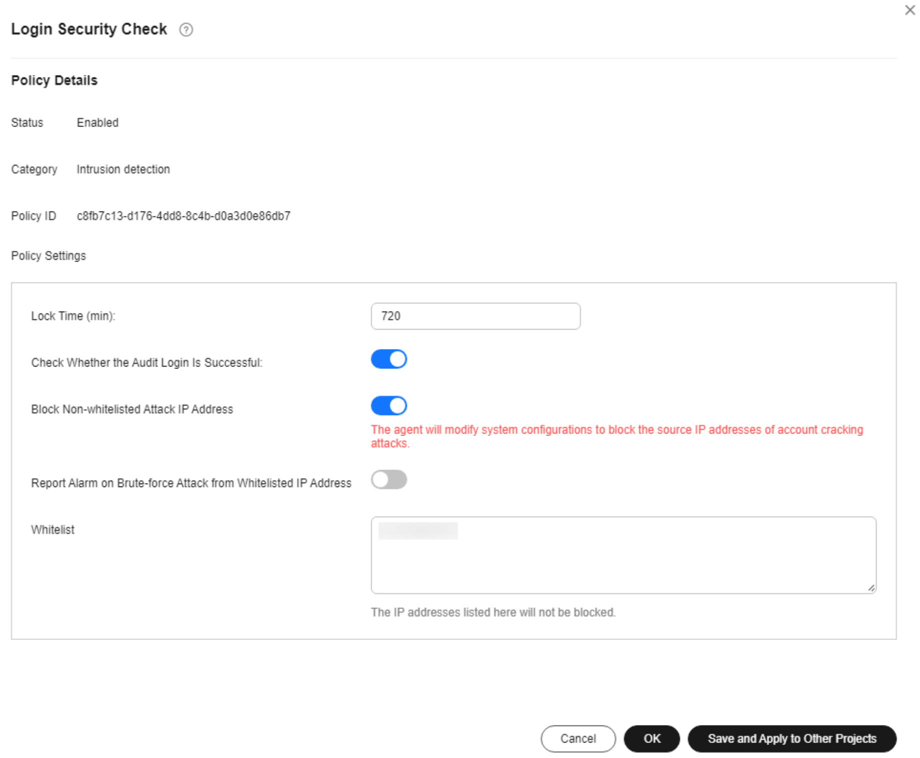
----End

Login Security Check

Step 1 Click **Login Security Check**.

Step 2 In the displayed **Login Security Check** page, modify the policy content. **Table 7-10** describes the parameters.

Figure 7-6 Modifying the security check policy



Login Security Check

Policy Details

Status Enabled

Category Intrusion detection

Policy ID c8fb7c13-d176-4dd8-8c4b-d0a3d0e86db7

Policy Settings

Lock Time (min): 720

Check Whether the Audit Login Is Successful: ●

Block Non-whitelisted Attack IP Address ●

The agent will modify system configurations to block the source IP addresses of account cracking attacks.

Report Alarm on Brute-force Attack from Whitelisted IP Address ○

Whitelist

The IP addresses listed here will not be blocked.

Table 7-10 Parameter description

Parameter	Description
Lock Time (min)	This parameter is used to determine how many minutes the IP addresses that send attacks are locked. The value range is 1 to 43200. Login is not allowed in the lockout duration.
Check Whether the Audit Login Is Successful	● After this function is enabled, HSS reports login success logs. – ●: enabled – ○: disabled
Block Non-whitelisted Attack IP Address	After this function is enabled, HSS blocks the login of brute force IP addresses (non-whitelisted IP addresses).
Report Alarm on Brute-force Attack from Whitelisted IP Address	● After this function is enabled, HSS generates alarms for brute force attacks from whitelisted IP addresses. – ●: enabled – ○: disabled

Parameter	Description
Whitelist	After an IP address is added to the whitelist, HSS does not block brute force attacks from the IP address in the whitelist. A maximum of 50 IP addresses or network segments can be added to the whitelist. Both IPv4 and IPv6 addresses are supported.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

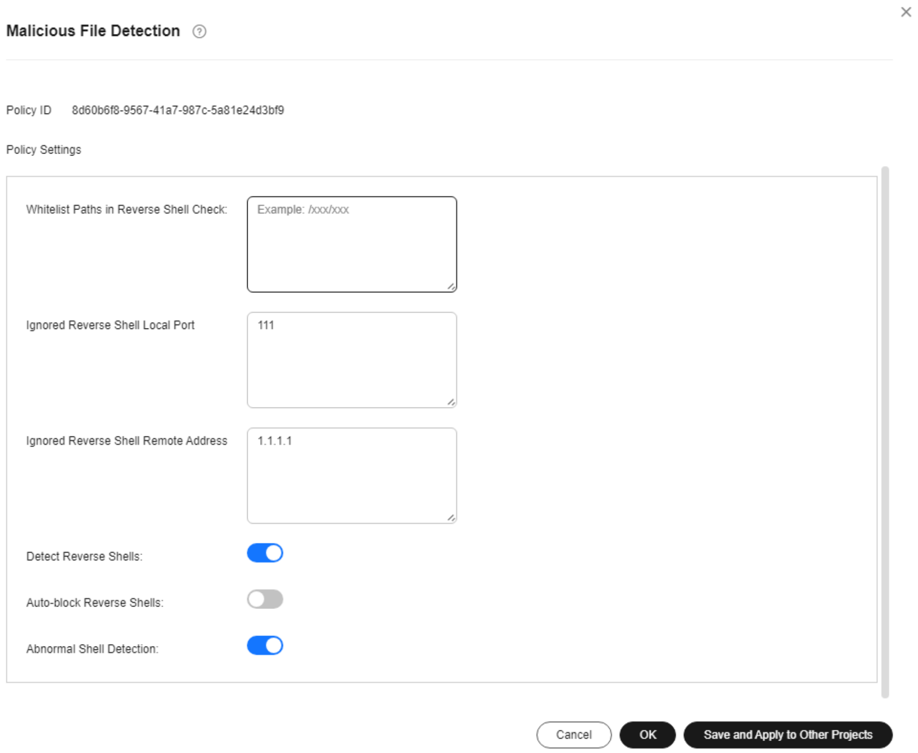
----End

Malicious File Detection

Step 1 Click **Malicious File Detection**.

Step 2 On the displayed page, modify the policy. For more information, see **Table 7-11**.

Figure 7-7 Modifying the malicious file detection policy



Malicious File Detection

Policy ID 8d60b6f8-9567-41a7-987c-5a81e24d3bf9

Policy Settings

Whitelist Paths in Reverse Shell Check: Example: /xxx/xxx

Ignored Reverse Shell Local Port 111

Ignored Reverse Shell Remote Address 1.1.1.1

Detect Reverse Shells: ●

Auto-block Reverse Shells: ○

Abnormal Shell Detection: ●

Table 7-11 Parameter description

Parameter	Description
Whitelist Paths in Reverse Shell Check	Process file path to be ignored in reverse shell detection Start with a slash (/) and end with no slashes (/). Occupy a separate line and cannot contain spaces.
Ignored Reverse Shell Local Port	Local ports that do not need to be scanned for reverse shells.
Ignored Reverse Shell Remote Address	Remote addresses that do not need to be scanned for reverse shells.
Detect Reverse Shells	● Detects reverse shells. You are advised to enable it. – : enabled – : disabled
Auto-block Reverse Shells	Specifies whether to enable automatic blocking of reverse shells. You are advised to enable this function. ● : enabled ● : disabled **NOTE** This parameter takes effect after the function of **Isolating and Killing Malicious Programs** is enabled.
Abnormal Shell Detection	● Detects abnormal shells. You are advised to enable it. – : enabled – : disabled

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Abnormal Process Behavior

Step 1 Click **Abnormal process behaviors**.

Step 2 In the displayed area, modify the settings as required. For more information, see **Table 7-12**.

Table 7-12 Parameter description

Parameter	Description	Example Value
Detection Mode	Select the method for abnormal process behavior detection. ● **Sensitive**: In-depth and full detection and scanning are performed on all processes, which may cause false positives. Suitable for cyber protection drills and key event assurance drills. ● **Balanced**: All processes are detected and scanned. The detection result accuracy and the abnormal process detection rate are balanced. Suitable for routine protection. ● **Conservative**: All processes are detected and scanned. This mode provides high detection result accuracy and low false positives. Suitable for scenarios with a large number of false positives.	Balanced

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

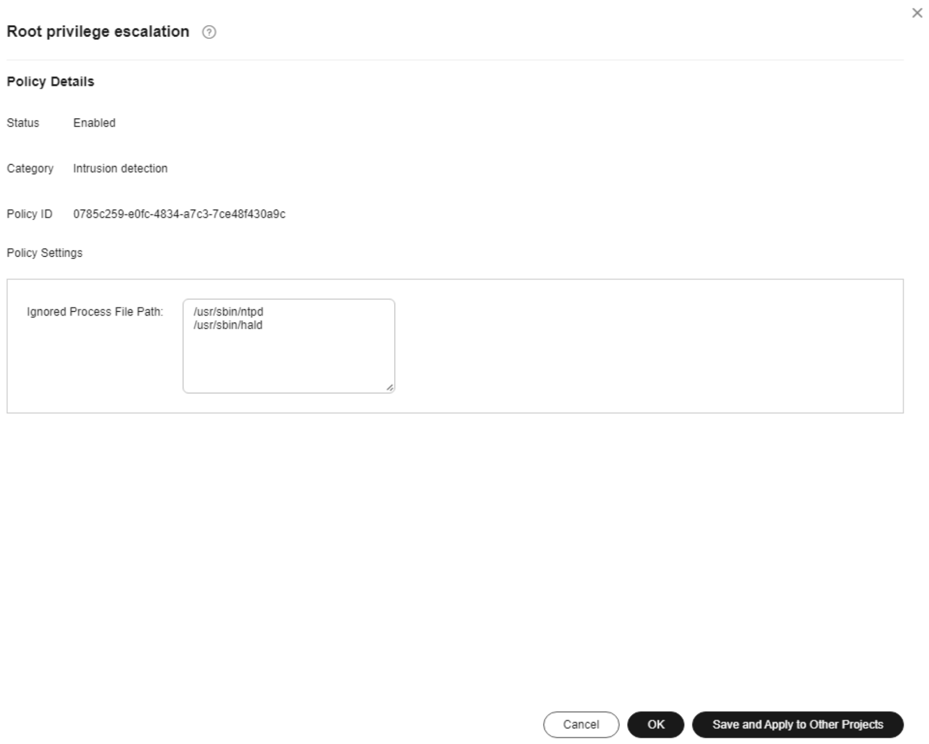
----End

Root Privilege Escalation Detection

Step 1 Click **Root privilege escalation**.

Step 2 In the displayed area, modify the settings as required. For more information, see **Table 7-13**.

Figure 7-8 Modifying the root privilege escalation policy



Root privilege escalation

Policy Details

Status Enabled

Category Intrusion detection

Policy ID 0785c259-e0fc-4834-a7c3-7ce48f430a9c

Policy Settings

Ignored Process File Path:

```
/usr/sbin/ntpd
/usr/sbin/hald
```

Table 7-13 Parameter description

Parameter	Description
Ignored Process File Path	Ignored process file path Start with a slash (/) and end with no slashes (/). Occupy a separate line and cannot contain spaces.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

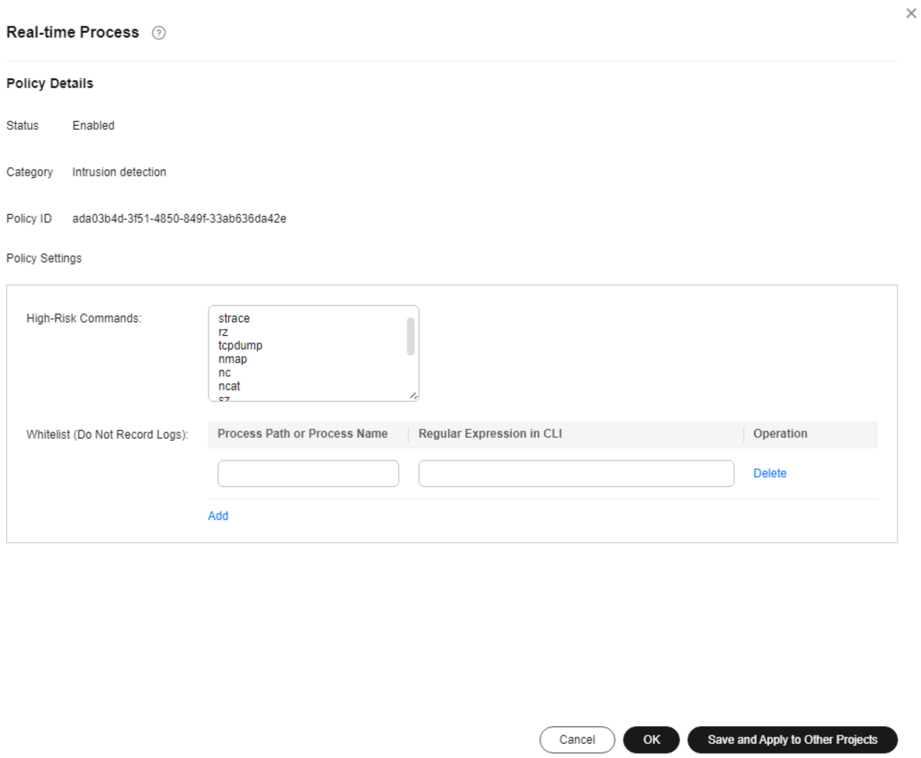
----End

Real-time Process

Step 1 Click **Real-time Process**.

Step 2 On the displayed page, modify the settings as required. For more information, see **Table 7-14**.

Figure 7-9 Modifying the real-time process policy



Real-time Process

Policy Details

Status Enabled

Category Intrusion detection

Policy ID ada03b4d-3f51-4850-849f-33ab636da42e

Policy Settings

High-Risk Commands:

```
strace
rz
tcpdump
nmap
nc
ncat
sz
```

Whitelist (Do Not Record Logs):

Process Path or Process Name	Regular Expression in CLI	Operation
		Delete

Table 7-14 Parameters for real-time process policy settings

Parameter	Description
High-Risk Commands	High-risk commands that contain keywords during detection. The command can contain only letters, numbers, hyphens (-), spaces, and special characters (/*\=>.:'"+-). **NOTE** Currently, built-in shell commands cannot be detected.
Whitelist (Do Not Record Logs)	Paths or programs that are allowed or ignored during detection. You can enter the regular expression of the command to be added to the whitelist. The command regular expression is optional. Example: ● Full path or program name of a process: /usr/bin/sleep ● Command regular expression: ^[A-Za-z0-9[:space:]\\*\\.\\\":_'\\(>=-]+$

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

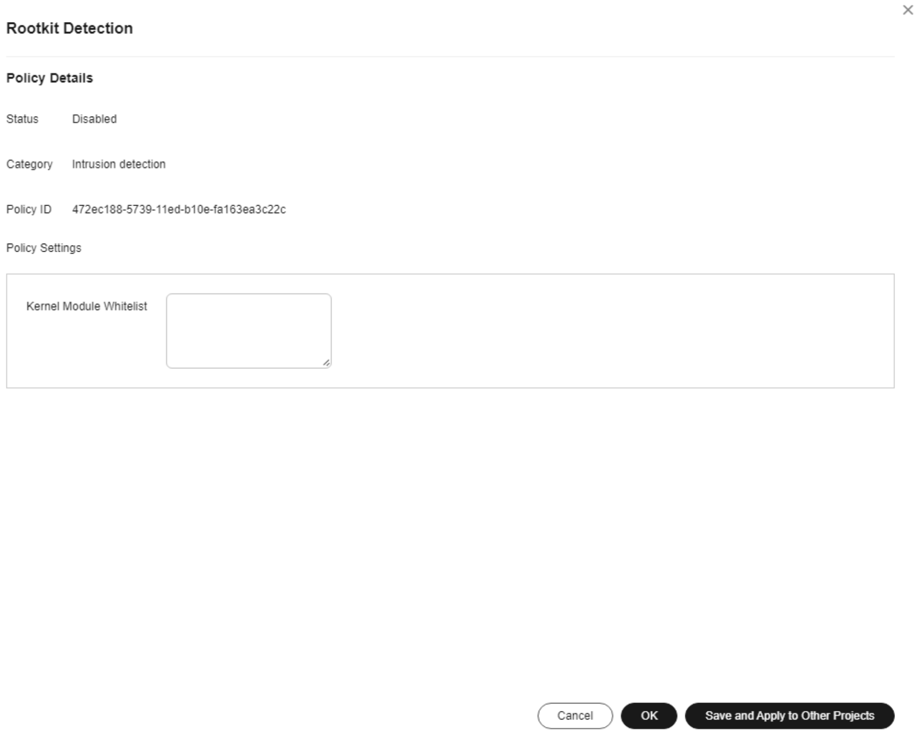
----End

Rootkit Detection

Step 1 Click **Rootkit Detection**.

Step 2 On the rootkit detection page, modify the policy content.

Figure 7-10 Modifying the rootkit detection policy



Rootkit Detection

Policy Details

Status Disabled

Category Intrusion detection

Policy ID 472ec188-5739-11ed-b10e-fa163ea3c22c

Policy Settings

Kernel Module Whitelist

Table 7-15 Parameter description

Parameter	Description	Example Value
Kernel Module Whitelist	Add the kernel modules that can be ignored during the detection. Up to 10 kernel modules can be added. Each module occupies a line.	xt_conntrack virtio_scsi tun

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

AV Detection

Step 1 Click **AV Detection**.

Step 2 On the **AV Detection** slide pane that is displayed, modify the settings as required. For details, see **Table 7-16**.

Table 7-16 AV detection policy parameters

Parameter	Description	Example Value
Real-Time Protection	After this function is enabled, AV detection is performed in real time when the current policy is executed. You are advised to enable this function. ● 🔵: enabled ● ⚪: disabled	🔵: enabled
Protected File Type	Type of the files to be checked in real time. ● **All**: Select all file types. ● **Executable**: Executable file types such as EXE, DLL, and SYS. ● **Compressed**: Compressed file types such as ZIP, RAR, and JAR. ● **Text**: Text file types such as PHP, JSP, HTML, and Bash. ● **OLE**: Composite file types such as Microsoft Office files (PPT and DOC) and saved email files (MSG). ● **Other**: File types except the preceding types.	All
Action	Handling method for the object detection alarms. ● **Automated handling**:Isolate high-risk virus files bu default. Report other virus files but do not isolate them. ● **Manual handling**: Report all the detected virus files but do not isolate them. You need to handle them manually.	Automated handling

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Container Information Collection

Step 1 Click **Container Information Collection**.

Step 2 On the **Container Information Collection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 7-17**.

NOTE

The whitelist has a higher priority than blacklist. If a directory is specified in both the whitelist and blacklist, it is regarded as a whitelisted item.

Table 7-17 Container information collection policy parameters

Parameter	Description	Example Value
Mount Path Whitelist	Enter the directory that can be mounted.	/test/docker or /root/* Note: If a directory ends with an asterisk (*), it indicates all the sub-directories under the directory (excluding the main directory). For example, if **/var/test/*** is specified in the whitelist, all sub-directories in **/var/test/** are whitelisted, excluding the **test** directory.
Mount Path Blacklist	Enter the directories that cannot be mounted. For example, **user** and **bin**, the directories of key host information files, are not advised being mounted. Otherwise, important information may be exposed.	

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Cluster Intrusion Detection

Step 1 Click **Cluster Intrusion Detection**.

Step 2 On the **Cluster Intrusion Detection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 7-18**.

Table 7-18 Cluster intrusion detection policy parameters

Parameter	Description	Example Value
Basic Detection Cases	Select basic check items as required.	Select all

Parameter	Description	Example Value
Whitelist	You can customize the types and values that need to be ignored during the detection. You can add and delete types and values as required. The following types are supported: ● IP address filter ● Pod name filter ● Image name filter ● User filter ● Pod tag filter ● Namespace filter NOTE Each type can be used only once.	Type: IP address filtering Value: 192.168.x.x

NOTE

After this policy is configured, you need to enable the log audit function and deploy the HSS agent on the management node (node where the APIServer is located) of the cluster to make the policy take effect.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Container Escape Detection

Step 1 Click **Container Escape**. The container escape policy details page is displayed.

Step 2 On the container escape page that is displayed, edit the policy content. For details about the parameters, see **Table 7-19**.

If no image, process, or POD needs to be added to the whitelist, leave the whitelist blank.

Table 7-19 Container escape detection policy parameters

Parameter	Description
Image Whitelist	Enter the names of the images that do not need to perform container escape behavior detection. An image name can contain only letters, numbers, underscores (_), and hyphens (-), and each name needs to be on a separate line. Up to 100 processes are allowed.

Parameter	Description
Process Whitelist	Enter the names of processes that do not need to perform container escape behavior detection. A process name can contain only letters, numbers, underscores (_), and hyphens (-), and each name needs to be on a separate line. Up to 100 processes are allowed.
Pod Whitelist	Enter the names of pods that do not need to perform container escape behavior detection. A pod name can contain only letters, numbers, underscores (_), and hyphens (-), and each name needs to be on a separate line. Up to 100 pods are allowed.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Container Information Module

Step 1 Click **Container Information Collection**.

Step 2 Modify the policy content as prompted. For details about the parameters related to the policy, see **Table 7-20**.

Table 7-20 Container information collection policy parameters

Parameter	Description
Custom Container Whitelist	Enter the container name that can be ignored during the detection. ● Simple names of containers can be configured based on Docker. HSS automatically performs fuzzy match. Other containers perform exact match based on their names. ● Enter each image whitelist on a separate line. Up to 100 whitelists are allowed.
Custom Image Organization Whitelist	Enter the organization name that can be ignored during the detection. Enter each image organization whitelist on a separate line. Up to 100 whitelists are allowed.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Container File Monitoring

NOTICE

If a monitored file path is under the mount path rather than the writable layer of the container on the server, changes on the file cannot trigger container file modification alarms. To protect such files, configure a **file protection policy**.

Step 1 Click **Container File Monitoring**.

Step 2 On the **Container File Monitoring** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 7-21**.

Table 7-21 Container file monitoring policy parameters

Parameter	Description	Example Value
Fuzzy match	Indicates whether to enable fuzzy match for the target file. You are advised to select this option.	Selected
Image Name	Name of the target image to be checked	test_bj4
Image ID	ID of the target image to be checked	-
File	Name of the file in the target image to be checked	/tmp/testw.txt

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Container Process Whitelist

Step 1 Click **Container Process Whitelist**.

Step 2 On the **Container Process Whitelist** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 7-22**.

Table 7-22 Container process whitelist policy parameters

Parameter	Description	Example Value
Fuzzy Match	Indicates whether to enable fuzzy match for the target file. You are advised to select this option.	Selected
Image Name	Name of the target image to be detected	test_bj4
Image ID	ID of the target image to be checked	-
Process	Path of the file in the target image to be checked	/tmp/testw

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Suspicious Image Behaviors

Step 1 Click **Suspicious Image Behaviors**.

Step 2 On the **Suspicious Image Behaviors** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 7-23**.

Table 7-23 Suspicious image behaviors policy parameters

Parameter	Description	Example Value
Rule Name	Name of a rule	-
Description	Brief description of a rule	-

Parameter	Description	Example Value
Template	● Configure templates based on different rules. The supported rules are as follows: – Image whitelist – Image blacklist – Image tag whitelist – Image tag blacklist – Create container whitelist – Create container blacklist – Container mount proc whitelist – Container seccomp unconfined – Container privilege whitelist – Container capability whitelist ● The parameters are described as follows: – **Exact match**: Enter the names of the images you want to check. Use semicolons (;) to separate multiple names. A maximum of 20 names can be entered. – **RegEx match**: Use regular expressions to match images. Use semicolons (;) to separate multiple expressions. A maximum of 20 expressions can be entered. – **Prefix match**: Enter the prefixes of the images you want to check. Multiple prefixes are separated by semicolons (;). A maximum of 20 prefixes can be entered. – **Tag Name**: Enter the tag and value of the images you want to check. A maximum of 20 tags can be added. – **Permission Type**: Specify permissions to be checked or ignored. For details about permissions, see **Table 7-24**.	-

Table 7-24 Abnormal image permissions

Permissions Name	Description
AUDIT_WRITE	Write records to kernel auditing log.
CHOWN	Make arbitrary changes to file UIDs and GIDs.
DAC_OVERRIDE	Bypass file read, write, and execute permission checks.

Permissions Name	Description
FOWNER	Bypass permission checks on operations that normally require the file system UID of the process to match the UID of the file.
FSETID	Do not clear set-user-ID and set-group-ID permission bits when a file is modified.
KILL	Bypass permission checks for sending signals
MKNOD	Create special files using mknod.
NET_BIND_SERVICE	Bind a socket to internet domain privileged ports (port numbers less than 1024).
NET_RAW	Use RAW and PACKET sockets.
SETFCAP	Set file capabilities.
SETGID	Make arbitrary manipulations of process GIDs and supplementary GID list.
SETPCAP	Modify process capabilities.
SETUID	Make arbitrary manipulations of process UIDs.
SYS_CHROOT	Use chroot to change the root directory.
AUDIT_CONTROL	Enable and disable kernel auditing; change auditing filter rules; retrieve auditing status and filtering rules.
AUDIT_READ	Allow reading audit logs via multicast netlink socket.
BLOCK_SUSPEND	Allow suspension prevention.
BPF	Allow creating BPF maps, loading BPF Type Format (BTF) data, retrieve JITed code of BPF programs, and more.
CHECKPOINT_RESTORE	Allow operations related to checkpoints and restoration.
DAC_READ_SEARCH	Bypass file read permission checks and directory read and execute permission checks.
IPC_LOCK	Lock memory (such as mlock, mlockall, mmap, and shmctl).
IPC_OWNER	Bypass permission checks for operations on System V IPC objects.
LEASE	Establish leases on arbitrary files
LINUX_IMMUTABLE	Set the FS_APPEND_FL and FS_IMMUTABLE_FL i-node flags.
MAC_ADMIN	Allow MAC configuration or state changes.
MAC_OVERRIDE	Override Mandatory Access Control (MAC).

Permissions Name	Description
NET_ADMIN	Perform various network-related operations.
NET_BROADCAST	Make socket broadcasts, and listen to multicasts.
PERFMON	Allow privileged system performance and observability operations using perf_events, i915_perf and other kernel subsystems.
SYS_ADMIN	Perform a range of system administration operations.
SYS_BOOT	Use reboot and kexec_load. Reboot and load a new kernel for later execution.
SYS_MODULE	Load and unload kernel modules.
SYS_NICE	Raise process nice value (nice, set priority) and change the nice value for arbitrary processes.
SYS_PACCT	Enable or disable process accounting.
SYS_PTRACE	Trace arbitrary processes using ptrace.
SYS_RAWIO	Perform I/O port operations (ipl and ioperm).
SYS_RESOURCE	Override resource limits.
SYS_TIME	Set the system clock (settimeofday, stime, and adjtimex) and real-time (hardware) clock.
SYS_TTY_CONFIG	Use vhangup. Employ various privileged ioctl operations on virtual terminals.
SYSLOG	Perform privileged syslog operations.
WAKE_ALARM	Trigger something that will wake up the system.

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Port Scan Detection

Step 1 Click **Port Scan Detection**.

Step 2 On the **Port Scan Detection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 7-25**.

Table 7-25 Port scan detection policy parameters

Parameter	Description	Example Value
Source IP Address Whitelist	Enter the IP address whitelist. Separate multiple IP addresses with semicolons (;).	test_bj4
Ports to Scan	Details about the port number and protocol type to be detected	-

Step 3 Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

----End

Self-protection

The self-protection policy protects HSS software, processes, and files from being damaged by malicious programs. You cannot customize the policy content.

7.1.4 Deleting a Policy Group

Preset policy groups cannot be deleted. You can delete custom policy groups of premium edition and container edition.

Constraints

After a policy group is deleted, the **Policy Group** column of the servers that were associated with the group will be blank. You need to deploy a policy group for a server again by referring to **Deploying a Protection Policy**.

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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Security Operations** > **Policies**

Step 4 Click **Delete** in the **Operation** column of the target policy.

You can also select multiple policies and click **Delete** in the upper left corner of the policy list to delete multiple policy groups in batches.

Step 5 Click **OK**.

----End

7.2 Viewing the Handling History

You can check the handling history of vulnerabilities and alarms, including their handlers and handling time.

Constraints

The basic edition does not support this function. For details about how to buy and upgrade HSS, see **Purchasing Quota** and **Upgrading Protection Quotas**.

Viewing the Handling History of all 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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Security Operations** > **Handling History**. The **Handling History** page is displayed.

Step 4 On the **Vulnerabilities** tab page displayed, view the handling history of all vulnerabilities.

- Viewing the vulnerability handling history of a specified enterprise project

  In the upper left corner of the **Handling History** page, select an enterprise project for **Enterprise Project** to view the handling history of server vulnerabilities in the enterprise project.

- Viewing the vulnerability handling history of a specified property

  In the search box above the vulnerability handling history list, enter a vulnerability type, vulnerability name, or server IP address, and click 🔍 to view the vulnerability handling history of a specified property.

----End

Checking the Alarm Handling History

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** > HSS.

Step 3 In the navigation pane on the left, choose **Security Operations** > **Handling History**.

Step 4 Click the **Alarms** tab and view the handling history of alarms.

- Checking the handling history of alarms under an enterprise project

  In the upper left corner of the **Handling History** page, select an enterprise project and check the handling history of server alarms under the project.

- Checking the handling history of alarms with specified attributes

In the search box above the alarm list, enter an alarm name, alarm severity, and attack ID, and click 🔍 to search for the alarms that meet the specified criteria.

----End

Viewing the Handling History of Virus Scanning

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Security Operations** > **Handling History**.

Step 4 Click the **Virus Scan** tab to view the handling history of the virus scan alarm event.

- View the handling history of virus scan under an enterprise project.

  In the upper left corner of the **Handling History** page, select an enterprise project and check the handling history of virus scan under the project.

- View the handling history of virus scan events with specified attributes.

  In the search box above the virus scan list, enter the virus name, virus file path, virus level, and virus type, and click 🔍 to view the handling history of virus scan events with specified attributes.

----End

8 Security Report

8.1 Security Report

8.1.1 Creating a Security Report

If the type and content of the existing report template cannot meet your requirements, you can customize a report.

Constraints

The enterprise, premium, WTP, or container edition 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** > **HSS**.

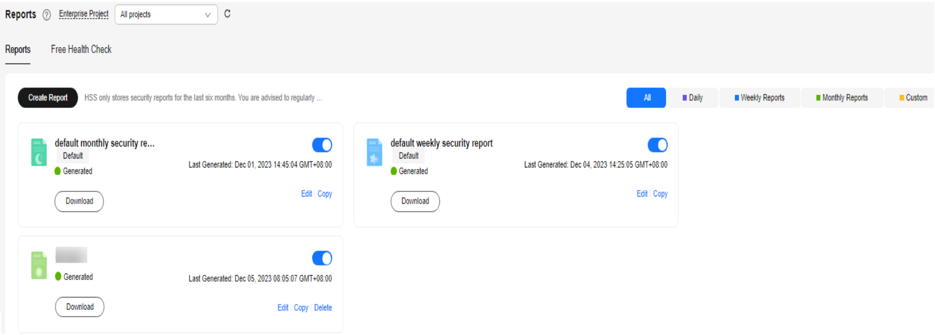
Step 3 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 8-1 Checking a security report



Reports ⓘ Enterprise Project All projects C

Reports | Free Health Check

Create Report HSS only stores security reports for the last six months. You are advised to regularly ...

All | Daily | Weekly Reports | Monthly Reports | Custom

default monthly security re...
Default
Generated
Last Generated: Dec 01, 2023 14:45:04 GMT+08:00
Download
Edit | Copy

default weekly security report
Default
Generated
Last Generated: Dec 04, 2023 14:25:05 GMT+08:00
Download
Edit | Copy

[redacted]
Generated
Last Generated: Dec 05, 2023 08:05:07 GMT+08:00
Download
Edit | Copy | Delete

Step 4 Create a report.

- Create a monthly or weekly security report based on templates.
  - Click **Copy** in the weekly or monthly report card to access the basic information configuration page.
- You can also customize the report period.
  - Click **Create Report** to access the basic information configuration page.

Step 5 Edit basic information of a report. For more information, see **Table 8-1**.

Table 8-1 Parameter description

Parameter	Description	Example Value
Report Name	Default report name	ecs security report
Report Type	Statistical period type of a report: ● **Daily**: 00:00 to 24:00 every day ● **Weekly Reports**: 00:00 on Monday to 24:00 on Sunday ● **Monthly Reports**: 00:00 on the first day to 24:00 on the last day of each month ● **Custom**: custom statistical period, which ranges from one day to three months ● All types of reports will be sent to the recipients the day after it is generated.	Monthly Reports
Schedule Delivery	Time when a report is automatically sent	-

Parameter	Description	Example Value
Send Report To	Security report recipients. - **Recipients specified in Message Center**: If you use Message Center settings, alarm notifications will be sent to the recipients specified in the **Security events** message type. You need to log in to the console and check the mailbox in the upper right corner. - **Recipients specified in SMN topic**: If you use SMN topic settings, you can create a topic and specify recipients for HSS. - **No need to send to email**: The report is not sent to the specified email address.	Recipients specified in SMN topic

Step 6 After confirming that the information is correct, click **Next** in the lower right corner of the page to configure the report.

Step 7 Select the report items to be generated in the left pane. You can preview the report items in the right pane. After confirming the report items, click **Save**, and enable security report subscription.

----End

8.1.2 Subscribing to a Security Report

This section provides guidance for you to quickly subscribe to weekly or monthly security reports using preset templates on the console. For details about how to customize a security report, see **Creating a Security Report**.

Constraints

The enterprise, premium, WTP, or container edition is enabled.

Precaution

- A security report is generated for all protected servers. You cannot specify a server and generate a security report for it.
- Subscription to security reports is free of charge, but the report content varies depending on the quota edition you use.

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** > **HSS**.

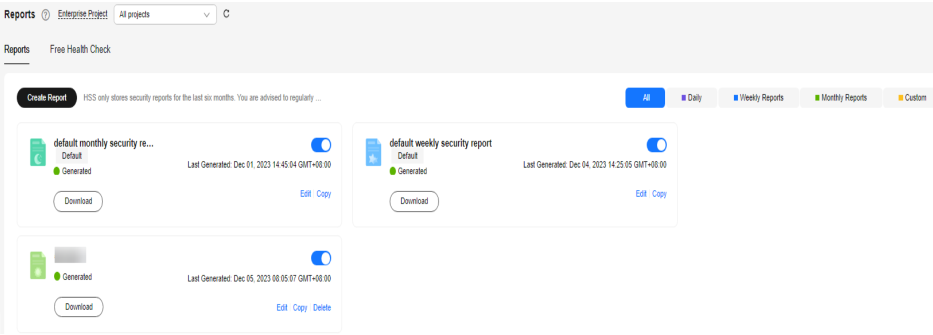
Step 3 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

NOTE

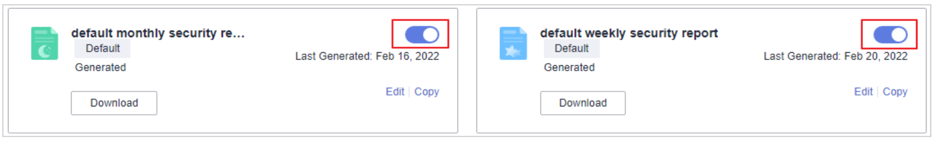
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 8-2 Checking a security report


Reports
Enterprise Project
All projects
Reports
Free Health Check
Create Report
HSS only stores security reports for the last six months. You are advised to regularly ...
All
Daily
Weekly Reports
Monthly Reports
Custom
default monthly security re...
Default
Generated
Last Generated: Dec 01, 2023 14:45:04 GMT+08:00
Edit | Copy
Download
default weekly security report
Default
Generated
Last Generated: Dec 04, 2023 14:25:05 GMT+08:00
Edit | Copy
Download
Generated
Last Generated: Dec 05, 2023 08:05:07 GMT+08:00
Download
Edit | Copy | Delete

Step 4 You can subscribe to monthly or weekly security reports. For details about how to edit a report, see **Editing a Report**.

Figure 8-3 Enabling security reports


default monthly security re...
Default
Generated
Last Generated: Feb 16, 2022
Edit | Copy
Download
default weekly security report
Default
Generated
Last Generated: Feb 20, 2022
Edit | Copy
Download

----End

8.1.3 Checking a Security Report

You can subscribe to **daily**, weekly, monthly, and **custom** reports, which are stored for six months. The reports show your server security trends and key security events and risks.

NOTE

- 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.
- After you subscribe to a report, it will be available for review and download the next day.

Constraints

The enterprise, premium, WTP, or container edition is enabled.

Security Report Overview

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** > **HSS**.

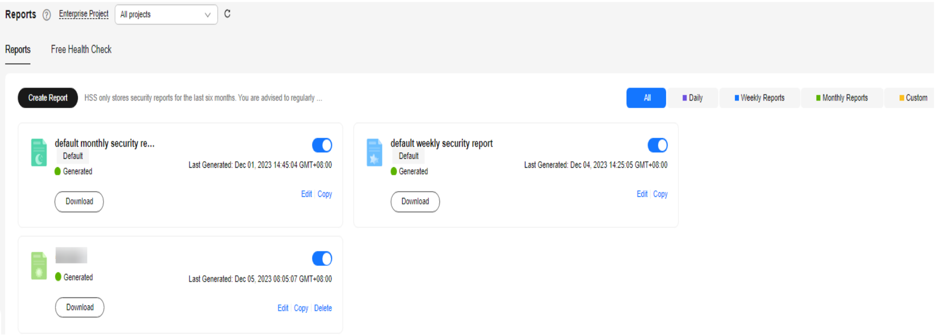
Step 3 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 8-4 Checking a security report



HSS only stores security reports for the last six months. You are advised to regularly ...

default monthly security re...
Default
Generated
Last Generated: Dec 01, 2023 14:45:04 GMT+08:00

default weekly security report
Default
Generated
Last Generated: Dec 04, 2023 14:25:05 GMT+08:00

[redacted]
Generated
Last Generated: Dec 05, 2023 08:05:07 GMT+08:00

Step 4 Click **Download** to go to the preview page. You can check the information of the target report and download or send it.

----End

Checking Report History

The report history stores the report sending details.

Step 1 In the upper right corner of the security report overview page, click **Report History** to check the report sending records.

Step 2 Check the report history on the displayed page, as shown in the following picture. For more information, see **Table 8-2**.

Table 8-2 Parameter description

Parameter	Description
Report Name	Name of a sent report.
Statistical Period	Statistical period of a sent report.

Parameter	Description
Report Type	Statistical period type of a sent report. ● Weekly Reports ● Monthly Reports ● Daily Reports ● Custom Reports
Sent	Time when the report is sent.

Step 3 Click **Download** in the **Operation** column to check historical reports. You can also preview and download the reports.

----End

8.1.4 Managing Security Reports

This section describes how to modify, cancel, or disable a subscribed report.

Constraints

The enterprise, premium, WTP, or container edition is enabled.

Editing a 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** > **HSS**.

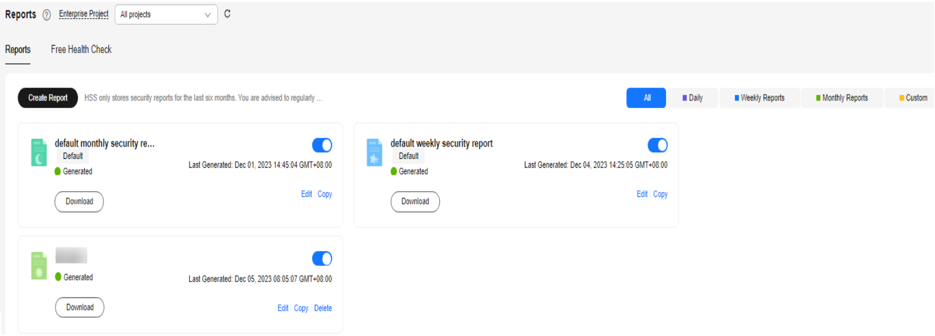
Step 3 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 8-5 Checking a security report



Reports ⓘ Enterprise Project: All projects

Reports | Free Health Check

Create Report — HSS only stores security reports for the last six months. You are advised to regularly ...

All | Daily | Weekly Reports | Monthly Reports | Custom

default monthly security re...
Default
Generated
Last Generated: Dec 01, 2023 14:45:04 GMT+08:00
Download
Edit | Copy

default weekly security report
Default
Generated
Last Generated: Dec 04, 2023 14:25:05 GMT+08:00
Download
Edit | Copy

[redacted]
Generated
Last Generated: Dec 05, 2023 08:05:07 GMT+08:00
Download
Edit | Copy | Delete

Step 4 Click **Edit** in the lower right corner of the target report.

Step 5 Edit basic information of a report. For more information, see **Table 8-3**.

Table 8-3 Parameter description

Parameter	Description	Example Value
Report Name	Default report name.	**default monthly security report**
Report Type	Name of the statistical period type of a report, which cannot be edited.	**Monthly Reports**
Schedule Delivery	Time when a report is automatically sent.	-
Send Report To	Mode to send the generated security reports: ● **Recipients specified in Message Center**: If you use Message Center settings, alarm notifications will be sent to the recipients specified in the **Security events** message type. You need to log in to the console and check the mailbox in the upper right corner. ● **Recipients specified in SMN topic**: If you use SMN topic settings, you can create a topic and specify recipients for HSS. ● **No need to send to email**: The report is not sent to the specified email address.	Recipients specified in SMN topic

Step 6 Confirm the information and click **Next** in the lower right corner of the page to configure the report.

Step 7 Select or deselect the report items in the pane on the left. You can preview the report items on the right. After confirming the report items, click **Save**. The report is changed successfully.

----End

Unsubscribing from a Report

Step 1 Log in to the management console and go to the HSS page.

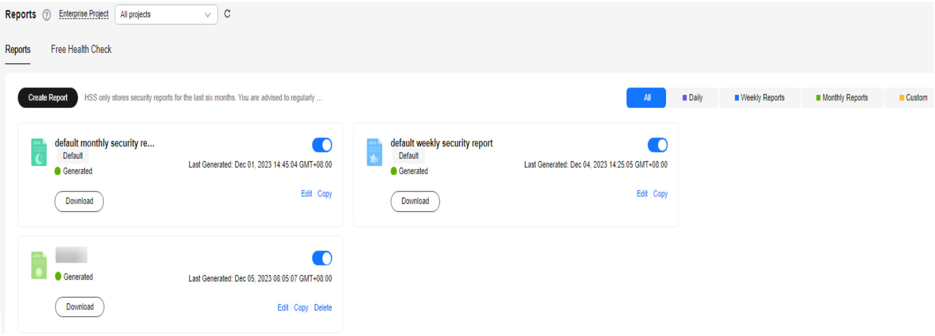
Step 2 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 8-6 Checking a security report



HSS only stores security reports for the last six months. You are advised to regularly ...

default monthly security re...
Default
Generated
Last Generated: Dec 01, 2023 14:45:04 GMT+08:00

default weekly security report
Default
Generated
Last Generated: Dec 04, 2023 14:25:05 GMT+08:00

[redacted]
Generated
Last Generated: Dec 05, 2023 08:05:07 GMT+08:00

Step 3 Toggle off the target report ( ).

----End

Deleting a Report

NOTE

Default security report templates **default monthly security report** and **default weekly security report** cannot be deleted.

Step 1 Log in to the management console and go to the HSS page.

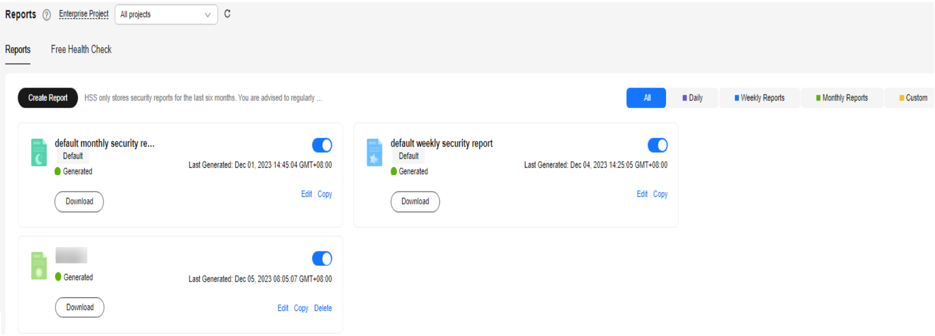
Step 2 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figure 8-7 Checking a security report



HSS only stores security reports for the last six months. You are advised to regularly ...

default monthly security re...
Default
Generated
Last Generated: Dec 01, 2023 14:45:04 GMT+08:00

default weekly security report
Default
Generated
Last Generated: Dec 04, 2023 14:25:05 GMT+08:00

[redacted]
Generated
Last Generated: Dec 05, 2023 08:05:07 GMT+08:00

Step 3 Click **Delete** in the lower right corner of the target report.

----End

8.2 Free Scan

Servers that are not protected by HSS are scanned for free. A security report on their vulnerabilities, unsafe passwords, and asset risks will be generated.

If you need to perform baseline check, application protection, web tamper protection, ransomware protection, intrusion detection, policy management, file integrity detection, and isolation and killing, you can **enable HSS**.

Free Scan

- Servers that are not protected by HSS are scanned for free in the early morning on each Monday.
- A free health check report is generated on the first day of each month. You can only view the report online but cannot download it.
- In the report, up to five results can be displayed for each check item. If a check item has fewer than five results, only half of them will be displayed.
- You can purchase HSS to enjoy advanced functions, such as real-time protection, report download, online vulnerability fix, and compliance assistance.

Procedure

Step 1 Log in to the management console.

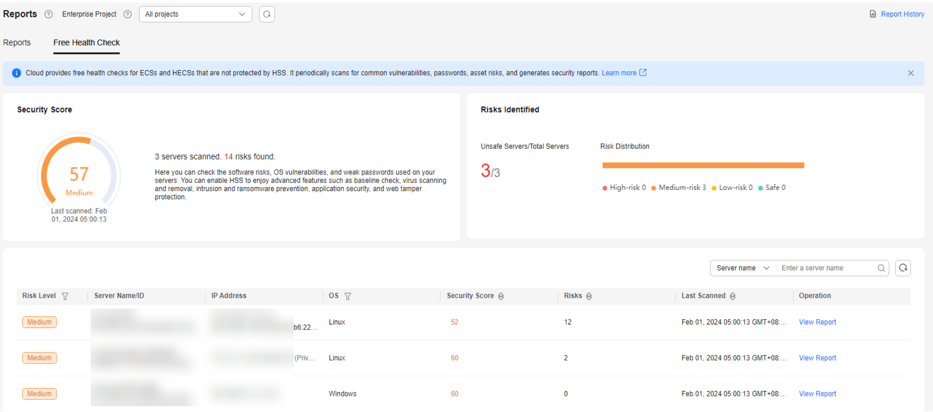
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Choose **Reports** and click the **Free Health Check** tab. Check the statistics of assets that are not protected.

NOTE

Only unprotected servers are displayed on this page.

Figure 8-8 Free health check



Cloud provides free health checks for ECSs and HECSs that are not protected by HSS. It periodically scans for common vulnerabilities, passwords, asset risks, and generates security reports. Learn more

Security Score

57
Medium
Last scanned: Feb 01, 2024 05:00:13

3 servers scanned. 14 risks found.

Here you can check the software risks, OS vulnerabilities, and weak passwords used on your servers. You can enable HSS to enjoy advanced features such as baseline check, virus scanning and removal, intrusion and ransomware prevention, application security, and web tamper protection.

Risks Identified

Unsafe Servers/Total Servers: 3/3

Risk Distribution: ● High-risk 0 ● Medium-risk 3 ● Low-risk 0 ● Safe 0

Risk Level	Server Name/ID	IP Address	OS	Security Score	Risks	Last Scanned	Operation
Medium	[redacted]	[redacted]	Linux	52	12	Feb 01, 2024 05:00:13 GMT+08:...	View Report
Medium	[redacted]	[redacted]	Linux	60	2	Feb 01, 2024 05:00:13 GMT+08:...	View Report
Medium	[redacted]	[redacted]	Windows	60	0	Feb 01, 2024 05:00:13 GMT+08:...	View Report

Step 4 In the **Operation** column of a server, click **View Report** to view the health check report online.

----End

9 Installation & Configuration

9.1 Agent Management

9.1.1 Viewing Agent Status

You can sort servers, check whether the agent is installed on them, and can install or uninstall the agent. On the console, you can find the agent installation instructions and the link to the agent package. For details about how to install an agent, see **Installing an Agent**.

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** > **HSS**.

Step 3 In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Check the agent status.

Step 5 Click **Add Asset from Other Cloud** to view the agent installation quick guide.

Step 6 Click **Agent Version Information** to view the latest version, earlier versions, and changes of the agent.

----End

9.1.2 Upgrading the Agent

HSS keeps improving its service capabilities, including but not limited to new features and defect fixes. Please upgrade your agent to the latest version in a timely manner to enjoy better service.

About the Upgrade

- Agent upgrade is free of charge.
- The upgrade does not affect the workloads on your cloud servers.
- You are advised to perform the upgrade during off-peak hours.

Manually Upgrading the Agent

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** > **HSS**.

Step 3 In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

Step 4 Click **Agents to Be Upgraded** and filter the servers whose agents are to be upgraded.

Step 5 In the **Operation** column of a server, click **Upgrade Agent**.

You can also select target servers in batches and click **Upgrade Agent** in the upper left corner of the server list to upgrade agents for the servers in batches.

Step 6 In the displayed dialog box, confirm the server whose agent is to be upgraded and click **OK** to start the automatic upgrade.

Step 7 After the upgrade completes, check the agent version. If the latest version agent is used, the upgrade is successful.

----End

Automatically Upgrading Agents

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** > **HSS**.

Step 3 In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.

NOTE

If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

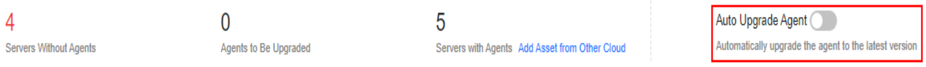
Step 4 Click ○ to enable automatic agent upgrade.

After this function is enabled, HSS checks the agent to be upgraded from 00:00 to 06:00 every day and automatically upgrades the agent to the latest version.

NOTE

The automatic upgrade can be performed only when the agent status is **Online**.

Figure 9-1 Enabling auto upgrade



----End

Related Operations

Installing an Agent

9.1.3 Uninstalling an Agent

If you no longer need to use HSS, uninstall the agent by following the instructions provided in this section. If the agent is uninstalled, HSS will stop protecting your servers and detecting risks.

Uninstallation Methods

Uninstallation Mode	Description
Uninstall the Online Agents	If the agent status of a server is **Online**, uninstall the agent by referring to **Uninstalling the Online Agents**.
Uninstall the Offline Agents	If the agent status of a server is **Offline**, uninstall the agent by referring to **Uninstall an Offline Agent**.

Uninstalling the Online Agents

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** > **HSS**.

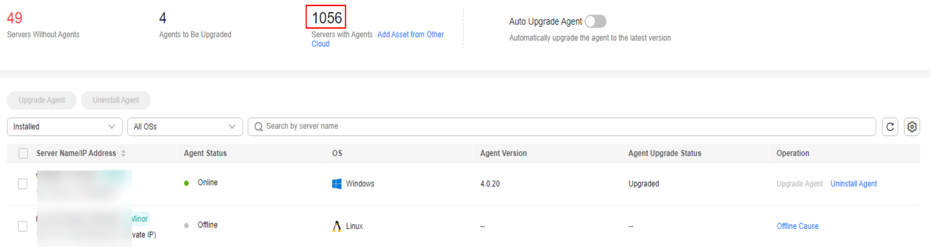
Step 3 In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.

NOTE

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Step 4 Click the value of **Servers with Agents** to view the list of servers where the agent has been installed. For details, see **Table 9-1**.

Figure 9-2 Viewing the online agent list



Server Name/IP Address	Agent Status	OS	Agent Version	Agent Upgrade Status	Operation
[redacted]	● Online	Windows	4.0.20	Upgraded	Upgrade Agent Uninstall Agent
[redacted] Minor vate IP)	● Offline	Linux	--	--	Offline Cause

Table 9-1 Online agent parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	EIP or private IP address of a server
OS	Server OS. Its value can be: ● **Linux** ● **Windows**
Agent Status	Agent status of a server. Its value can be: ● **Online**
Agent Version	Version of the agent installed on the target server.
Agent Upgrade Status	The agent upgrade status.

Step 5 Click **Uninstall Agent** in the **Operation** column of a server. In the dialog box that is displayed, confirm the uninstallation information and click **OK**.

If you need to uninstall the agent in batches, you can select servers and click **Uninstall Agent** above the list.

----End

Uninstall an Offline Agent

- **Uninstalling the Linux agent**

  a. Log in to the server from which you want to uninstall the agent and run the following command to switch to user root:

     su - root

  b. In any directory, run the following command to uninstall the agent:

NOTE

Do not run the uninstallation command in the **/usr/local/hostguard/** directory. You can run the uninstallation command in any other directory.

- For EulerOS, CentOS and Red Hat, or other OSs that support RPM installation, run the **rpm -e hostguard** command.
- For Ubuntu and Debian OSs, or other OSs that support DEB installation, run the **dpkg -P hostguard** command.

If information similar to the following is displayed, the agent has been successfully uninstalled. If the uninstallation fails, go to the **step 3**.

```
Stopping Hostguard...
Hostguard stopped
Hostguard uninstalled.
```

c. (Optional) If the agent fails to be uninstalled in **step 2**, perform the following operations to uninstall the agent:

- For OSs that support RPM installation, such as EulerOS, CentOS, and Red Hat.
  1) Run the following command to delete the installation record:

     rpm -e --justdb hostguard
  2) Run the following command to check whether there are hostguard processes:

     ps -ef | grep hostguard

     If there are residual processes, run the **kill -9 PID** command to kill all residual processes.
  3) Run the following command to check whether the **/usr/local/hostguard** directory exists:

     ll /usr/local/hostguard

     If the directory exists, run the **rm -rf /usr/local/hostguard** command to delete it.
  4) Run the following command to check whether the **/etc/init.d/hostguard** file exists:

     ll /etc/init.d/hostguard

     If the file exists, run the **rm -f /etc/init.d/hostguard** command to delete the file.
- For OSs that support DEB installation, such as Ubuntu and Debian.
  1) Run the following command to check whether there are hostguard processes:

     ps -ef | grep hostguard

     If there are residual processes, run the **kill -9 PID** command to kill all residual processes.
  2) Run the following command to check whether the **/usr/local/hostguard** directory exists:

     ll /usr/local/hostguard

     If the directory exists, run the **rm -rf /usr/local/hostguard** command to delete it.

3) Run the following command to check whether the **/etc/init.d/hostguard** file exists:

   ll /etc/init.d/hostguard

   If the file exists, run the **rm -f /etc/init.d/hostguard** command to delete the file.

- **Uninstalling the Windows agent**
  a. Log in to the server that you want to uninstall the agent.
  b. Click **Start** and choose **Control Panel** > **Programs**. Then select **HostGuard** and click **Uninstall**.

     NOTE

     - Alternatively, go to the **C:\Program File\HostGuard** directory and double-click **unins000.exe** to uninstall the program.
     - If you have created a folder for storing the agent shortcut under the **Start** menu when installing the agent, you can also choose **Start** > **HostGuard** > **Uninstall HostGuard** to uninstall HostGuard.

  c. In the **Uninstall HostGuard** dialog box, click **Yes**.
  d. (Optional) Restart the server.
     ▪ If you have enabled WTP, you need to restart the server after uninstalling the agent. In the **Uninstall HostGuard** dialog box, click **Yes** to restart the server.
     ▪ If you have not enabled WTP, you do not need to restart the server. In the **Uninstall HostGuard** dialog box, click **No** to skip server restart.

- **Windows**
  a. Remotely log in to the Windows server where the agent is to be uninstalled.
  b. Go to **C:\Program File\HostGuard** on the Windows server.
  c. Double-click the **unins000.exe** file to uninstall the agent.
  d. In the **HostGuard Uninstall** dialog box, click **Yes** to delete HostGuard and all its components.
  e. (Optional) Restart the server.
     ▪ If you have enabled WTP, you need to restart the server after uninstalling the agent. In the **HostGuard Uninstall** dialog box, click **Yes** to restart the server.
     ▪ If you have not enabled WTP, you do not need to restart the server. In the **HostGuard Uninstall** dialog box, click **No** to skip server restart.
  f. If the **C:\Program Files\HostGuard** directory does not exist on the Windows server, the agent has been uninstalled.

Related Operations

Installing an Agent

9.2 Account Management

9.2.1 Account Management Overview

HSS provides secure and reliable cross-account data aggregation and resource access capabilities. If your accounts are managed by an organization, you can use HSS to protect the workload of all member accounts in the organization in a unified manner.

- HSS provides unified security protection for servers of all member accounts in an organization, including asset management, vulnerability detection and fixing, baseline check, and intrusion detection.
- HSS provides unified security protection for containers of all member accounts in an organization.

To protect the workload security of organization member accounts through HSS, perform the following operations:

1. **Adding an Account to an Organization**
2. **Viewing Account Management**

For details about the organization service, see **Overview of Organizations**.

9.2.2 Adding an Account to an Organization

This section describes how to add an account to an organization to perform workload security protection.

Prerequisites

- You have created an organization. For details, see **Creating an Organization**.
- You have configured HSS as a trusted service. For details, see **Enabling or Disabling a Trusted Service**.
- The current account is the organization administrator or the delegated administrator.

Constraints

Not all regions support the account management function. For details, see **Function Overview**.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Installation & Configuration** and click the **Account Management** tab. On the displayed page, click **Add Account**.

Step 4 On the dialog box that is displayed, select an account from the **Available Accounts** tree. The account is automatically added to the **Selected Accounts** area on the right. Confirm the information and click **OK**.

NOTE

The added accounts belong to the same organization. For details about organization accounts, see **Overview of an Account**.

Step 5 The account is added successfully and is displayed in the account list.

----End

9.2.3 Viewing Security Risks of Organization Member Accounts

On the **Account Management** tab page, you can view the organization member accounts that have been added to HSS for workload protection and the workload protection details of the accounts.

Viewing Account Management

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Installation & Configuration** and click the **Account Management** tab. On the displayed page, view the list of all accounts. For more information, see **Parameter description**.

Table 9-2 Parameter description

Parameter	Description
Account Name	Account name
Project Name	Region to which the account belongs
Servers	Number of servers under an account
Vulnerabilities (Last 24 hours)	Number of vulnerabilities on servers in the last 24 hours
Unsafe Settings (Last 24 hours)	Number of unsafe settings on servers in the last 24 hours
Alarms (Last 24 hours)	Number of security alarms on servers in the last 24 hours

----End

Deleting an Account

Step 1 Click **Delete** in the **Operation** column of the target account.

Step 2 In the dialog box that is displayed, confirm the information and click **OK**.

----End

9.3 Plug-in Settings

9.3.1 Plug-Ins Overview

You can install and manage plug-ins.

Plug-in Type

Currently, only Docker plug-ins can be managed.

Docker Plug-in Application Scenarios

If container protection is enabled and you want to use the image blocking function, you need to **install the Docker plug-in**.

The Docker plug-in provides the image blocking capability. It can prevent the startup of container images that have high-risk vulnerabilities or do not comply with security standards in the Docker environment.

You can configure image blocking in the following scenarios:

- To enhance the security of container images and prevent the risks caused by the use of untrusted or outdated images, you can configure an **image blocking policy** to specify the level of vulnerabilities to be blocked or the whitelist.
- If you need to comply with the security requirements of certain industries or regulations, such as PCI DSS and CIS, you can **configure an image blocking policy** to specify the security baseline or compliance check items to be blocked.
- If you need to implement the best practices of container DevSecOps and embed security check and defense into each phase of the container lifecycle, you can **configure an image blocking policy** to enhance security from source to devices.

9.3.2 Viewing Plug-in Details

You can view the details about the plug-ins used by servers.

You can install, upgrade, and uninstall plug-ins as required.

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** > **HSS**.

Step 3 In the navigation pane on the left, choose **Installation & Configuration** and click the **Plug-in Settings** tab to view details about all plug-ins. For more information, see **Table 9-3**.

By default, all servers are displayed in the plug-in list. If a plug-in is installed on a server, the plug-in details are displayed. If no plug-ins are installed on a server, the plug-in information is empty.

Table 9-3 Docker plug-in list parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	Server IP address
OS	Type of the OS running on the server
Plug-in Name	Name of the plug-in installed on the server.
Plug-in Version	Name of the plug-in installed on the server.
Plug-in Status	Current status of the plug-in. ● **Created**: The plug-in has been created but has not been started. ● **Running**: The plug-in is running properly. ● **Paused**: The plug-in is paused. ● **Restarting**: The plug-in is being restarted. ● **Removing**: The plug-in is being deleted. ● **Exited**: The plug-in has been stopped. ● **Dead**: The plug-in cannot be started or has been deleted.
Plug-in Upgrade Status	Plug-in upgrade status. ● **Not upgraded**: The plug-in has not been upgraded to the latest version. ● **Upgrading**: The plug-in is being upgraded. ● **Upgraded**: The plug-in has been upgraded. ● **Upgrade failed**: The plug-in failed to be upgraded.

----End

9.3.3 Installing a Plug-in

If container protection is enabled and you want to use the image blocking function, install the Docker plug-in by following the instructions provided in this section.

Constraints

- Only Docker containers are supported. Containerd containers are not supported.
- The Docker engine version is 18.06.0 or later.
- The Docker API version is 1.38 or later.
- Only Linux servers are supported.
- Only the x86 and Arm hardware architectures are supported.
- The HSS container edition has been enabled.
- Currently, only Huawei Cloud online servers are supported.

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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Installation & Configuration** and click the **Plug-in Settings** > **Docker plug-in** tab. Click **Plug-in installation guide**, obtain the installation commands from the slide-out panel, and click **Copy**.

Step 4 Remotely log in to the server where the plug-in is to be installed as the **root** user.

- 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 PuTTY or Xshell, to log in to the server and install the plug-in on the server as user **root**.

Step 5 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 6 Create **linux-host-list.txt**, which will contain the server private IP addresses where the agent is to be installed:

Command syntax:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
Or
echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

To specify multiple IP addresses, write multiple commands, each in a separate line.

Example:

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

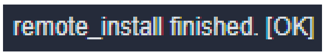
Step 7 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 8 Copy the batch installation commands to the command terminal and press **Enter**.

NOTE

If the installation package cannot be downloaded, check to ensure the DNS can resolve the domain name in the installation command.

Step 9 If **remote_install finished. [OK]** is displayed, the installation is successful. Wait for 3 to 5 minutes and choose **Installation & Configuration** and click the **Plug-in Settings** tab to check the Docker plug-in status of the panel server.



```
remote_install finished. [OK]
```

----End

9.3.4 Upgrading a Plug-in

You can upgrade plug-ins of a target server.

Constraints

- Only Docker containers are supported. Containerd containers are not supported.
- The Docker engine version is 18.06.0 or later.
- The Docker API version is 1.38 or later.
- Only Linux servers are supported.
- Only the x86 and Arm hardware architectures are supported.
- The HSS container edition has been enabled.
- Currently, only Huawei Cloud online servers are supported.

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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Installation & Configuration** and click the **Plug-in Settings** > **Docker plug-in** tab. Click **Plug-in upgrade guide**, obtain the upgrade commands from the slide-out panel, and click **Copy**.

Step 4 Remotely log in to the server where the plug-in is to be upgraded as the **root** user.

- 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 PuTTY or Xshell, to log in to the server and upgrade the plug-in on the server as user **root**.

Step 5 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 6 Create **linux-host-list.txt**, which will contain the server private IP addresses where the plug-in is to be upgraded:

Command syntax:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
Or echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

To specify multiple IP addresses, write multiple commands, each in a separate line.

Example:

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

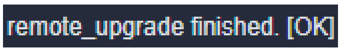
Step 7 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 8 Copy the batch upgrade commands to the command box and press **Enter**. The upgrade starts automatically.

NOTE

If the installation package cannot be downloaded, check to ensure the DNS can resolve the domain name in the installation commands.

Step 9 If **remote_upgrade finished. [OK]** is displayed, the upgrade is successful. Wait for 3 to 5 minutes and choose **Installation & Configuration** and click the **Plug-in Settings** tab to check the Docker plug-in status of the panel server.



```
remote_upgrade finished. [OK]
```

----End

9.3.5 Uninstalling a Plug-in

Constraints

- Only Docker containers are supported. Containerd containers are not supported.
- The Docker engine version is 18.06.0 or later.
- The Docker API version is 1.38 or later.
- Only Linux servers are supported.
- Only the x86 and Arm hardware architectures are supported.
- The HSS container edition has been enabled.
- Currently, only Huawei Cloud online servers are supported.

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** > **HSS**.

Step 3 In the navigation tree on the left, choose **Installation & Configuration** and click the **Plug-in Settings** > **Docker plug-in** tab. Click **Plug-in uninstallation guide**, obtain the uninstallation commands from the slide-out panel, and click **Copy**.

Step 4 Remotely log in to the server where the plug-in is to be uninstalled as the **root** user.

- 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 PuTTY or Xshell, to log in to the server and uninstall the plug-in on the server as user **root**.

Step 5 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 6 Create **linux-host-list.txt**, which will contain the server private IP addresses where the plug-in is to be uninstalled:

Command syntax:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
Or echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

To specify multiple IP addresses, write multiple commands, each in a separate line.

Example:

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

Step 7 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 8 Copy the batch uninstallation commands to the command box and press **Enter**. The uninstallation starts automatically.

Step 9 If **remote_uninstall finished. [OK]** is displayed, the uninstallation is successful. Wait for 3 to 5 minutes and choose **Installation & Configuration** and click the **Plug-in Settings** tab to check the Docker plug-in status of the panel server.

```
remote_uninstall finished. [OK]
```

----End

10 Audit

10.1 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 10-1 lists HSS operations recorded by CTS.

Table 10-1 HSS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Unignoring a port	hss	notIgnorePortStatus
Ignoring a port	hss	ignorePortStatus
Unignoring configuration check items	hss	notIgnoreCheckRuleStat
Ignoring configuration check items	hss	ignoreCheckRuleStat
Retrying a baseline check	hss	runBaselineDetect
Unbinding quota	hss	cancelHostsQuota
Disabling container protection	hss	closeContainerProtect-Status
Enabling container protection	hss	openContainerProtect-Status
Unblocking an IP address	hss	changeBlockedIp
Handling an event	hss	changeEvent
Canceling the isolation of a file	hss	changeIsolatedFile

Operation	Resource Type	Trace Name
Removing an alarm from whitelist	hss	removeAlarmWhiteList
Adding Login Whitelist	hss	addLoginWhiteList
Removing Login Whitelist	hss	removeLoginWhiteList
Adding a server group	hss	addHostsGroup
Adding servers to a group	hss	associateHostsGroup
Modifying a server group	hss	changeHostsGroup
Deleting a server group	hss	deleteHostsGroup
Disabling HSS	hss	closeHostsProtectStatus
Enabling HSS	hss	openHostsProtectStatus
Uninstalling an agent	hss	uninstallAgents
Scanning an image	hss	runImageScan
Synchronizing the image list from SWR	hss	runImageSynchronize-Task
Updating and scanning an SWR image	hss	runSwrImageScan
Performing a security check again	hss	resetRiskScore
Adding a policy group	hss	addPolicyGroup
Removing a policy group	hss	deletePolicyGroup
Applying a policy group	hss	deployPolicyGroup
Modifying a policy	hss	modifyPolicyDetail
Modifying a policy group	hss	modifyPolicyGroup
Disabling automatic isolation and killing	hss	closeAutoKillVirusStatus
Enabling automatic isolation and killing	hss	openAutoKillVirusStatus
Configure common login IP addresses	hss	modifyLoginCommonIp
Configure common login locations	hss	modifyLoginCommonLocation
Configuring the SSH login whitelist	hss	modifyLoginWhiteIp
Fixing a vulnerability	hss	changeVulStatus

Operation	Resource Type	Trace Name
Adding a protected directory	hss	addHostProtectDirInfo
Adding a privileged process	hss	addPrivilegedProcessInfo
Adding a scheduled protection setting	hss	addTimingOffConfigInfo
Removing a remote backup server	hss	deleteBackupHostInfo
Removing a protected directory	hss	deleteHostProtectDirInfo
Removing a privileged process	hss	deletePrivilegedProcessInfo
Deleting scheduled protection settings	hss	deleteTimingOffConfigInfo
Configuring the scheduled protection period	hss	setDateOffConfigInfo
Modifying the status of a protected directory	hss	setProtectDirSwitchInfo
Enabling or disabling dynamic WTP	hss	setRaspSwitch
Configuring a remote backup server	hss	setRemoteBackupInfo
Enabling or disabling scheduled protection	hss	setTimingOffSwitchInfo
Disabling WTP	hss	closeWtpProtectionStatus
Enabling WTP	hss	openWtpProtectionStatus
Modifying a remote backup server	hss	updateBackupHostInfo
Modifying a protected directory	hss	updateHostProtectDirInfo
Modifying a privileged process	hss	updatePrivilegedProcessInfo
Modifying the Tomcat bin directory	hss	updateRaspPathInfo
Modifying the scheduled protection period	hss	updateTimingOffConfigInfo

10.2 Querying Real-Time Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.

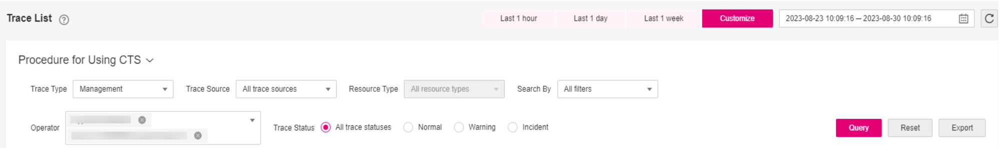
- **Operator**: Select one or more operators from the drop-down list.
- **Trace Status**: Select **normal**, **warning**, or **incident**.
  - **normal**: The operation succeeded.
  - **warning**: The operation failed.
  - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
- Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.

5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
   - Enter any keyword in the search box and click 🔍 to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
   - Click ↻ to view the latest information about traces.
   - Click ⚙ to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & GovernanceManagement & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces, as shown in **Figure 10-1**. The following filters are available:

Figure 10-1 Filters



Trace List

Last 1 hour | Last 1 day | Last 1 week | Customize | 2023-08-23 10:09:16 – 2023-08-30 10:09:16

Procedure for Using CTS

Trace Type: Management

Trace Source: All trace sources

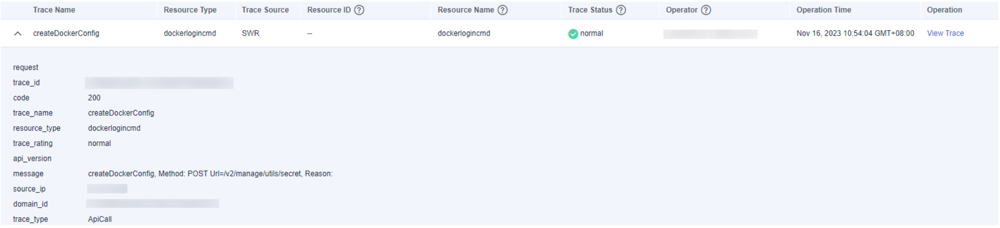
Resource Type: All resource types

Search By: All filters

Operator: [redacted]

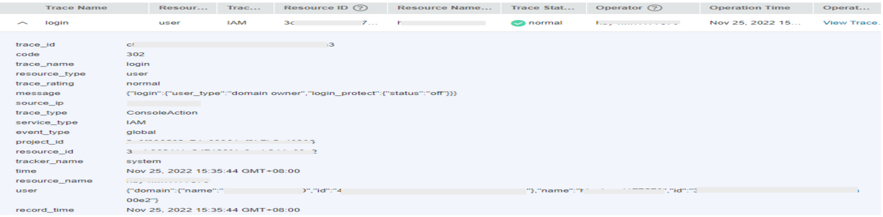
Trace Status: ● All trace statuses ○ Normal ○ Warning ○ Incident

   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: You can query traces generated during any time range in the last seven days.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
   - Click ⟳ to view the latest information about traces.
8. Click ⌄ on the left of a trace to expand its details.



	Trace Name	Resource Type	Trace Source	Resource ID ⓘ	Resource Name ⓘ	Trace Status ⓘ	Operator ⓘ	Operation Time	Operation
^	createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	✓ normal	[redacted]	Nov 16, 2023 10:54:04 GMT+08:00	View Trace

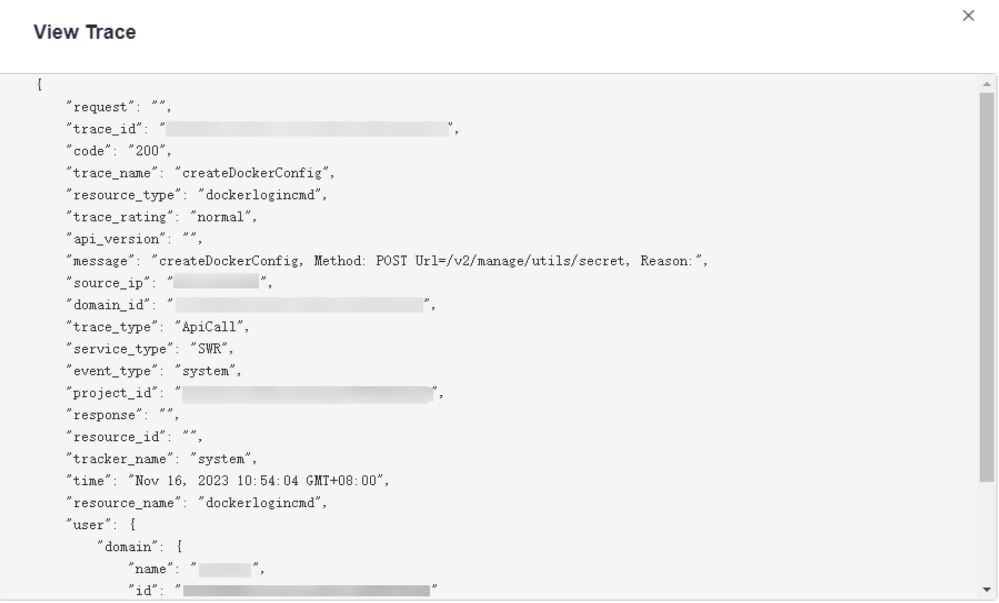
request	
trace_id	[redacted]
code	200
trace_name	createDockerConfig
resource_type	dockerlogincmd
trace_rating	normal
api_version	
message	createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:
source_ip	[redacted]
domain_id	[redacted]
trace_type	ApiCall



	Trace Name	Resour...	Trac...	Resource ID ⓘ	Resource Name...	Trace Stat...	Operator ⓘ	Operation Time	Operat...
^	login	user	IAM	3c[redacted]7...	r[redacted]	✓ normal	[redacted]	Nov 25, 2022 15...	View Trace.

trace_id	c[redacted]3
code	302
trace_name	login
resource_type	user
trace_rating	normal
message	{"login":{"user_type":"domain owner","login_protect":{"status":"off"}}}
source_ip	[redacted]
trace_type	ConsoleAction
service_type	IAM
event_type	global
project_id	[redacted]
resource_id	3[redacted]2
tracker_name	system
time	Nov 25, 2022 15:35:44 GMT+08:00
resource_name	[redacted]
user	{"domain":{"name":"[redacted]","id":"4[redacted]"},"name":"[redacted]","id":"3[redacted]00e2"}
record_time	Nov 25, 2022 15:35:44 GMT+08:00

9. Click **View Trace** in the **Operation** column. The trace details are displayed.



View Trace

```
{
    "request": "",
    "trace_id": "[redacted]",
    "code": "200",
    "trace_name": "createDockerConfig",
    "resource_type": "dockerlogincmd",
    "trace_rating": "normal",
    "api_version": "",
    "message": "createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:",
    "source_ip": "[redacted]",
    "domain_id": "[redacted]",
    "trace_type": "ApiCall",
    "service_type": "SWR",
    "event_type": "system",
    "project_id": "[redacted]",
    "response": "",
    "resource_id": "",
    "tracker_name": "system",
    "time": "Nov 16, 2023 10:54:04 GMT+08:00",
    "resource_name": "dockerlogincmd",
    "user": {
        "domain": {
            "name": "[redacted]",
            "id": "[redacted]"
```

10. For details about key fields in the trace structure, see **Trace Structure**section "Trace References" > "Trace Structure" and **Example Traces**section "Trace References" > "Example Traces".
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

11 Monitoring

11.1 HSS Monitoring Metrics

Feature Description

This section describes the HSS namespaces, function metrics, and dimensions reported to Cloud Eye. You can view HSS function metrics and alarms by using the Cloud Eye console or calling APIs.

Namespace

SYS.HSS

Metrics

Table 11-1 HSS monitoring metrics

ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
host_num	Total Servers	Total number of servers	≥ 0	Server	300s
unprotected_host_num	Unprotected Servers	Servers for which protection is not enabled	≥ 0	Server	300s

ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
risky_host_num	Unsafe Servers	Number of servers where risks are detected	≥ 0	Server	300s
uninstalled_or_offline_agent_num	Servers Without Agent Running	Number of servers where no agent is installed or the agent is offline	≥ 0	Server	300s

Dimensions

Table 11-2 Dimension list

key	Value
hss_enterprise_project_id	Enterprise project ID.

11.2 Configuring a Monitoring Alarm Rule

You can set HSS alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring period, and whether to send notifications. This helps you learn the HSS protection status in a timely manner.

Procedure

Step 1 Log in to the management console.

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

Step 3 Hover your mouse over ≡ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 On the displayed page, set the parameters as prompted.

For more information, see **Creating an Alarm Rule**. The key parameters are as follows:

- **Name**: Alarm rule name. The system generates a name, which you can modify.
- **Resource Type**: **Host Security Service**
- **Dimension**: **Host Security**
- **Monitoring Scope**: Scope of resources that the alarm rule applies to. You can select **All resources** or **Specific resources**.
- **Method**: Select **Associate template**, **Use existing template**, or **Configure manually**.

  NOTE

  After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.
- **Alarm Policy**: Policy for triggering an alarm.

Step 7 Configure the alarm notification.

To send alarm notifications via email, SMS, HTTP, or HTTPS, toggle on **Alarm Notification** ().

For more information, see **Creating an Alarm Rule**. The key parameters are as follows:

Step 8 Click **Create**.

----End

11.3 Viewing Monitoring Metrics

Cloud Eye can monitor the servers protected by HSS. You can view HSS monitoring metrics on the management console.

Procedure

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

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

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Host Security Service**.

Step 5 In the **Operation** column of an enterprise project ID, click **View Metric** to view the server protection metric details of the project.

----End

12 Permissions Management

12.1 Creating a User and Granting Permissions

This section describes IAM's fine-grained permissions management for your HSS 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 specific 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 12-1**).

Prerequisite

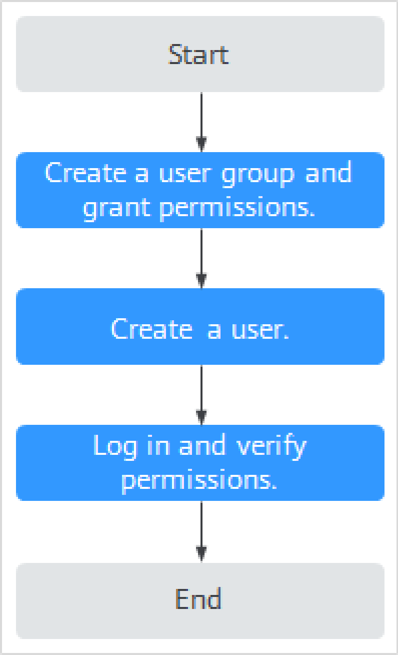
Before authorizing permissions to a user group, you need to know which HSS permissions can be added to the user group. **Table 12-1** describes the policy details.

Table 12-1 System-defined permissions supported by HSS

Role/Policy Name	Description	Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS	System-defined role	● It 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**, **BSS Administrator**, and **TMS ReadOnlyAccess** 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. – **TMS ReadOnlyAccess**: a system-defined policy that grants read-only access to TMS.
HSS FullAccess	All HSS permissions	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. **SMN ReadOnlyAccess**: a system-defined policy that grants read-only access to SMN.
HSS ReadOnlyAccess	Read-only permission for HSS	System-defined policy	**SMN ReadOnlyAccess**: a system-defined policy that grants read-only access to SMN.

Authorization Process

Figure 12-1 Process for granting permissions


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

1. **Create a user group and assign permissions**. On the IAM console, grant the **HSS Administrator** permission.
2. **Create a user and add it to the group**. On the IAM console, add the user to the group created in **1**.
3. **Log in** and verify permissions.

   Log in to the HSS console as the created user, and verify that the user only has read permissions for HSS.

   In **Service List** on the 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.

12.2 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 **HSS Actions**.

You can create custom policies using one of the following methods:

- Visual editor: Select cloud services, actions, resources, and request conditions. You do not need to have knowledge of the policy syntax.
- JSON: Create a policy in JSON format or edit the JSON strings of 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 policies 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 policies

  A custom policy can contain the actions of multiple services that are of the project-level type. The following is a policy with multiple statements:

  ```
  {
          "Version": "1.1",
          "Statement": [
                  {
                          "Effect": "Allow",
                          "Action": [
                                  "hss:hosts:list"
                          ]
                  },
                 {
                          "Effect": "Allow",
                          "Action": [
                                  "hss:hosts:switchVersion",
                                  "hss:hosts:manualDetect",
                                  "hss:manualDetectStatus:get"
                          ]
                  }
          ]
  }
  ```

12.3 HSS 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 policies or roles to these groups. The user then inherits permissions from the groups it is a member of. This process is called authorization. After authorization, the user 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. IAM uses policies to perform fine-grained authorization. A policy defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

HSS 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. The following are related concepts:

- Permissions: Allow or deny certain operations.
- Actions: Specific operations that are allowed or denied.
- Dependent actions: When assigning permissions for an action, you also need to assign permissions for the dependent actions.

HSS supports the following actions that can be defined in custom policies:

Actions describes the HSS actions, such as querying the HSS list, enabling or disabling HSS for a server, and manual detection.

Actions

Permission	Action	Related Action
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	-

Permission	Action	Related Action
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	-
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	-

Permission	Action	Related Action
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	-
Configure common login locations	hss:commonLocations:set	-
Query common login locations	hss:commonLocations:list	-
Configure common login IP addresses	hss:commonIPs:set	-
Query common login IP addresses	hss:commonIPs:list	-
Configure the login IP address whitelist	hss:whiteIps:set	-
Query the login IP address whitelist	hss:whiteIps:list	-
Configure weak passwords	hss:weakPwds:set	-
Query weak passwords	hss:weakPwds:get	-
Configure web paths	hss:webDirs:set	-
Query web paths	hss:webDirs:get	-
Obtain the list of servers where 2FA is enabled	hss:twofactorAuth:list	-
Enable 2FA	hss:twofactorAuth:set	-
Enable or disable automatic isolation and killing of malicious programs	hss:automaticKillMp:set	-

Permission	Action	Related Action
Query the programs that have been automatically isolated and killed	hss:automaticKillMp:get	-
Query the agent download address	hss:installAgent:get	-
Uninstall an agent	hss:agent:uninstall	-
Query HSS alarms	hss:alertConfig:get	-
Configure 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	-
Configure backup servers	hss:wtpBackup:set	-
Query backup servers	hss:wtpBackup:get	-
Configure protected directories	hss:wtpDirectorys:set	-
Query the protected directory list	hss:wtpDirectorys:list	-
Query WTP records	hss:wtpReports:list	-
Configure privileged processes	hss:wtpPrivilegedProcess:set	-
Query the privileged process list	hss:wtpPrivilegedProcesses:list	-
Configure a protection mode	hss:wtpProtectMode:set	-
Query the protection mode	hss:wtpProtectMode:get	-
Configure a protected file system	hss:wtpFilesystems:set	-
Query the protected file system list	hss:wtpFilesystems:list	-
Configure scheduled protection	hss:wtpScheduledProtections:set	-
Query scheduled protection	hss:wtpScheduledProtections:get	-

Permission	Action	Related Action
Configure WTP alarms	hss:wtpAlertConfig:set	-
Query WTP alarms	hss:wtpAlertConfig:get	-
Query WTP statistics	hss:wtpDashboard:get	-
Query policy group	hss:policy:get	-
Configure a policy group	hss:policy:set	-
Query the detected intrusion list	hss:event:get	-
Perform operations on intrusions	hss:event:set	-
Query server groups	hss:hostGroup:get	-
Configure 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	-

13 (Optional) Managing Enterprise Projects

13.1 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**.

13.2 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 the WTP 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 and Compliance** > HSS. The HSS page is displayed.

Step 3 Choose **Asset Management** > **Servers & Quota** and click **Quotas**. The server protection quotas are displayed.

Step 4 In the quota list, select a quota whose **Usage Status** is **Idle** and click **Bind Server**.

Step 5 Select servers in the **Bind Server** dialog box.

Step 6 Click **OK**. The **Protection Status** of the server will change to **Enabled**.

----End

Binding Quotas to Containers

Perform the following steps to bind the container 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 and Compliance** > HSS. The HSS page is displayed.

Step 3 Choose **Asset Management** > **Containers & Quota** and click **Protection Quotas**. The server protection quotas are displayed.

Step 4 In the quota list, select a quota whose **Usage Status** is **Idle** and click **Bind Server**.

Step 5 Click the **Nodes** tab. Locate the target server and click **Enable Protection** in the **Operation** column.

NOTE

The status of the server to be protected must be **Normal**, and the agent status must be **Online**.

Step 6 Select servers in the **Bind Server** dialog box.

In the displayed dialog box, select **Yearly/Monthly**, read the *Container Guard Service Disclaimer*, and select **I have read and agreed to Container Guard Service Disclaimer**.

The quota can be allocated in the following ways:

- **Select a quota randomly**: Let the system allocate the quota with the longest remaining validity to the server.
- Select a quota ID and allocate it to a server.

Step 7 Click **OK**. The **Protection Status** of the server will change to **Enabled**.

----End

A Change History

Released On	Description
2024-03-25	This issue is the twenty-first official release. Added: - **Access Guide** - **Dynamic Port Honeypot** - **Creating a Security Group Policy (Cloud Native Network 2.0)** - **Managing Security Group Policy (Cloud Native Network 2.0)** - **Managing Isolated Files** Optimized: - **Exporting the Baseline Check Report**: Added support for exporting password complexity policy detection results. - **Creating a Policy**: Added the description of the dynamic bait switch. - **Scanning for Viruses**: Added support for automatic isolation virus scanning and removal. - **Server Alarms**: Added support for manual isolation and killing of web shell. Added the description of automatic isolation and killing. - **Configuring Policies**: Optimized the web shell detection, file protection, login security detection, malicious file detection, abnormal process behavior, root privilege escalation, real-time process, rootkit detection, asset discovery, configuration detection, and port scanning detection policies. Added the container information policy. The policy modification can be applied to other projects when selecting all projects.

Released On	Description
2024-02-02	This is the twentieth official release. Optimized: ● **Dashboard**: Added the operation description to the security score module and splitting the score deduction standard table. ● **Vulnerability Scan**: Modified the description of scan modes. ● **Baseline Inspection**: Adjusted the document structure. ● **Policy Management**: Adjusted the document structure.

Released On	Description
2023-12-21	This issue is the nineteenth official release. Added: - **Collecting Server Asset Fingerprints** - **Collecting Container Asset Fingerprints** - **Ignoring a Server** - **SWR Enterprise Edition Image** - **Exporting the Container Node List** - **Exporting the Protection Quota List** - **WTP Overview** - **Virus Scan** - **Exporting Server Alarms** - **Exporting Container Alarms** Optimized: - **Installing an Agent**: Added the agent overview and updated the description about agent installation operations. - **Alarm Notifications**: Optimized the alarm notification item table. - **Common Security Configuration**: Server login protection, malicious program isolation and removal, and two-factor authentication are described in separate sections. - **Deploying a Protection Policy**: Supported the deployment of container edition policies. - **Local Images**: Modified the information about the server associated with the local image. The full scan progress can be viewed. - **Managing SWR Private Images**: The full scan progress can be viewed, and the baseline check result can be exported. - **Managing SWR Shared Images**: The full scan progress can be viewed, and the baseline check result can be exported. - **Binding a Protection Quota**: Supported automatic quota binding. - **Vulnerability Management**: Supported emergency vulnerability scan. - **Baseline Inspection Overview**: Weak password detection supported Windows passwords. - **Handling Server Alarms**: The alarm whitelist rules supported remote IP addresses and user names. - **Configuring Policies**: Deleted the detection break time from the weak password detection policy, and added the ignorable information to the malicious file detection policy. - **Upgrading the Agent**: Supported automatic upgrade.

Released On	Description
	● **SWR Image Repository Vulnerabilities**: Added application vulnerability scan and optimized the vulnerability list.
2023-10-27	This is the eighteenth official release. Added: ● **Managing Cluster Agents** ● **Application Process Control** ● **Container Cluster Protection** ● **Monitoring** ● **Exporting Server Alarms** ● **Exporting Container Alarms** ● **Checking the Alarm Handling History** Optimized: ● Revised **Dashboard**. ● Added the following alarm types to **Server Alarms**: suspicious process execution, suspicious process file access, abnormal outbound connection, and port forwarding ● Added the following alarm types to **Container Alarm Events**: hacker tool, file privilege escalation, important file change, abnormal process behavior, suspicious command execution, user password theft, abnormal outbound connection, and port forwarding ● Ransomware prevention and ransomware backup can be separately enabled in **Ransomware Prevention**. ● User-defined rules can be added to the alarm whitelist and duplicate alarms can be handled in batches in **Handling Server Alarms**. ● User-defined rules can be added to the alarm whitelist and duplicate alarms can be handled in batches in **Handling Container Alarms**. ● Backup before vulnerability fixing is enabled in **Handling Vulnerabilities**.

Released On	Description
2023-07-25	This issue is the seventeenth official release. Added: ● **Container Firewalls** ● **Managing the System User Whitelist** ● **Viewing Container Information** ● **Handling Risk Containers** ● **Viewing Vulnerability Handling History** Optimized: ● **Login Security Check**: Added the configuration of brute force cracking whitelist. ● **Viewing Protection Quotas**: Supported viewing the servers associated with container quotas. ● **Viewing and Processing Baseline Check Results**: Added the difference description about MySQL versions. ● **Adding a Protected Directory**: Added the description about restrictions on excluded subdirectories and exporting protected directories. ● **Binding a Protection Quota**: Supported container quota binding. ● **Unbinding a Protection Quota**: Supported container quota unbinding. ● **Viewing and Processing Baseline Check Results**: Added the description of selecting different policies and viewing detection results. ● **Local Images**: Supported exporting vulnerability reports. ● **Managing SWR Private Images**: Supported exporting vulnerability reports, software compliance check, and base image information detection. ● **Managing SWR Shared Images**: Supported vulnerability report export and security scanning. ● **Container Alarm Events**: Supported detecting and reporting alarms for process privilege escalation, brute force cracking, unauthorized system user accounts, and execution of high-risk commands. ● **Malicious File Detection**: Supported automatic blocking of reverse shells. ● **Overview**: Added automatic self-protection. ● **Enabling Alarm Notifications**: Added the uninstalled agent alarm to the daily alarm notification. ● **Restoring Server Data**: Added the description of the backup purposes.

Released On	Description
	- **Vulnerability Management**: Optimized the operation process and supported adding vulnerabilities to the whitelist. - **Server Fingerprints**: Supported the middleware, web applications, and databases running on Windows. - **Container Fingerprints**: Supported accounts, databases, clusters, services, workloads, and containers. - Supported real-time manual update of the container asset information. Clusters, services, workloads, and containers are supported.
2023-06-15	This issue is the sixteenth official release. Optimized: - Added vulnerability detection for a single server in **Vulnerability Scan**. - Added the operation of viewing vulnerabilities on a single server in **Viewing Vulnerability Details**.
2023-06-01	This is the fifteenth official release. Changed the name of HSS advanced edition to professional edition.
2023-05-24	This is the fourteenth official release. Optimized: - Optimized **Servers Importance Management**. - Optimized constraints in **Container Images**. - Optimized **Viewing Plug-in Details**.
2023-04-27	This issue is the thirteenth official release. Added: - 2.4.3.2-Vulnerability Scan (Automatic) - **Purchasing a Backup Vault** Optimized: Optimized prerequisites in **Enabling Ransomware Prevention**.

Released On	Description
2023-03-31	This issue is the eleventh official release. Added the description about: ● The functions and policies supported by the advanced edition. ● Detection capabilities such as AV detection and HIPS detection in policy groups. ● New types of intrusion detection alarms, such as Trojan, viruses, and worms. ● The honeypot detection capability for Windows servers. ● Server assets update (manual). ● Unified account management. ● User-defined intervals in asset policies. ● Plugin installation
2023-01-18	This is the tenth official release. Added the following sections: ● **Local Images** ● **Managing SWR Shared Images** ● **Viewing Container Asset Fingerprints** ● **Managing Application Protection Policies** ● **Adding a Privileged Process** ● **Installing the Agent on Linux Servers in Batches (One-Click on the Console)** ● **Upgrading the Agent** Added the following content: ● The malicious file policy of the HSS enterprise edition supported reverse shell detection. ● The program list and package names can be viewed. ● The detection time and period can be customized for asset discovery policies. ● Rootkit alarms ● Risks in the baseline configuration can be rectified in one-click mode.
2022-12-10	This is the ninth official release. Modified: ● **Viewing and Handling Ransomware Protection Events** ● **Enabling Ransomware Prevention** ● **Managing Ransomware Prevention Policies** ● **Disabling Ransomware Prevention**

Released On	Description
2022-11-10	This is the eighth official release. Added the following sections: **Free Scan** **Vulnerability Scan**
2022-10-11	This is the seventh official release. Added **Upgrading Protection Quotas**.
2022-09-30	This is the sixth official release. Added the following sections: Enabling Protection **Disabling Protection** **Installing the Agent on Linux Servers in Batches (One-Click on the Console)**
2022-09-20	This is the fifth official release. Added the basic edition (yearly/monthly) on the purchase page.
2022-08-31	This is the fourth official release. Modified the description about the basic edition. The basic edition can be used free of charge within a specific period.
2022-07-28	This is the third official release. Added the application protection function. This function is available in the following regions: CN-Hong Kong, AP-Bangkok, and AP-Singapore. Ransomware prevention is supported in Windows.
2022-07-05	This issue is the second official release. Added description about specifying asset importance. Added description about exporting baseline check items. Added description about detecting application vulnerabilities.
2022-05-30	This issue is the first official release.