Host Security Service

FAQs

Issue 01

Date 2024-09-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 About HSS

1.1 What Is Host Security?

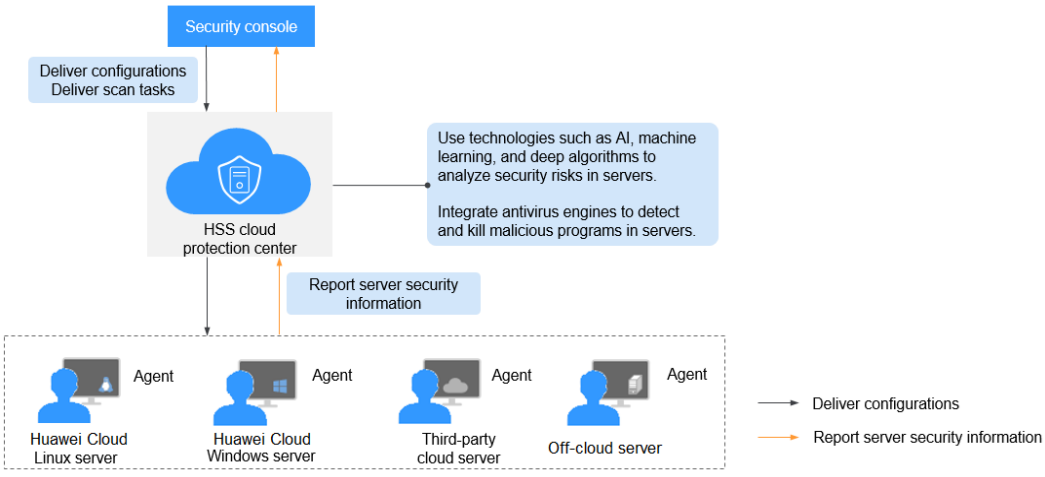
Host Security Service (HSS) helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

How HSS Works

Install the HSS agent on your servers, and you will be able to check the server security status and risks in a region on the HSS console.

Figure 1-1 shows the working principles of HSS.

Figure 1-1 Working principles



The functions and working processes of HSS components are described as follows:

Table 1-1 Components

Component	Description
Management console	A visualized management platform, where you can apply configurations in a centralized manner and view the protection status and scan results of servers in a region.
HSS cloud protection center	• Analyzes security risks in servers using AI, machine learning, and deep learning algorithms. • Integrates multiple antivirus engines to detect and kill malicious programs in servers. • Receives configurations and scan tasks sent from the console and forwards them to agents on the servers. • Receives server information reported by agents, analyzes security risks and exceptions on servers, and displays the analysis results on the console.
Agent	• Communicates with the HSS cloud protection center via HTTPS and WSS. Port 10180 is used by default. • Scans all servers every early morning; monitors the security status of servers; and reports the collected server information (including non-compliant configurations, insecure configurations, intrusion traces, software list, port list, and process list) to the cloud protection center. • Blocks server attacks based on the security policies you configured. **NOTE** • If no agent is installed or the agent installed is abnormal, the HSS is unavailable. • The agent can be installed on Huawei Cloud Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), on-premises IDC servers, and third-party cloud servers. • Select the agent and installation command suitable for your OS. • The HSS agent can be used for all editions, including container security and Web Tamper Protection (WTP). You only need to install the agent once on the same server.

1.2 What Is Container Security?

Container Security Service (CGS) scans vulnerabilities and configuration information in images, helping enterprises detect container risks that cannot be found using conventional security software. CGS also provides functions such as container process whitelist, container file monitoring, container information collection, and container escape detection to reduce risks.

1.3 What Is Web Tamper Protection?

Web Tamper Protection (WTP) monitors website directories in real time, backs up files, and restores tampered files using the backup. WTP protects your websites from Trojans, illegal links, and tampering.

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.

This section describes the operation process and main functions of WTP. See **Figure 1-2** and **Table 1-2**.

Figure 1-2 WTP operation process

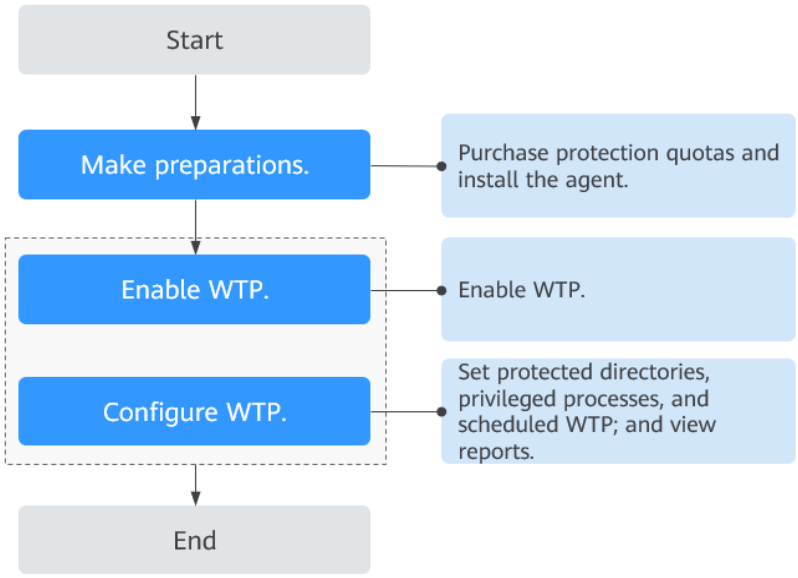


Table 1-2 WTP operation process and function description

Type	Operation	Description and Reference
Preparations	--	If no VDC operator account is available, contact an operations administrator to create a VDC.
Getting Started with WTP	Applying for Quota	Apply for WTP quota.
	Installing an Agent	The agent is provided by HSS. It runs scan tasks to scan all servers, monitors server security, and reports collected server information to the cloud protection center. You can enable WTP only after the agent is installed.

Type	Operation	Description and Reference
	Parameters required for configuring 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.
	Enabling HSS	Allocate a quota to a server and enable HSS for the server.
Enable WTP	Adding a Protected Directory	Add a directory to be protected by WTP.
	Create remote backup	By default, HSS backs up the files from the protected directories to the local backup directory you specified when you added protected directories. To protect the local backup files from tampering, you must enable the remote backup function.
	Adding a privileged process	After 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.
	Set scheduled WTP protection	You can schedule WTP protection to allow website updates in specific periods.
	Enabling dynamic WTP	Dynamic WTP protects your data while Tomcat is running, detecting dynamic data tampering in databases.
	View WTP reports	After WTP is enabled, HSS will immediately check the protected directories you specified. You can check records about detected tampering.

1.4 What Are the Relationships Between Images, Containers, and Applications?

- An image is a special file system. It provides programs, libraries, resources, configuration files and other files required for a running container. An image also contains some configuration parameters (such as anonymous volumes, environment variables, and users) prepared for a running container. An image does not contain any dynamic data, and its content is unchangeable after creation.

- The relationship between the image and container is similar to that between the class and instance in the program design. An image is static, and a container is the entity for a running image. A container can be created, started, stopped, deleted, and suspended.
- Multiple containers can be started for an image.
- An application may include one or a set of containers.

1.5 How Do I Use HSS?

To use the HSS, perform the following steps:

Step 1 **Purchase protection quotas**.

Step 2 **Install the agent**.

You can enable HSS after installing the agent.

Step 3 **Enable alarm notifications**.

After alarm notifications are enabled, you can receive alarm notifications sent by HSS to learn about security risks facing the server. Without this function, you have to log in to the management console to view alarms.

Step 4 **Enable HSS**.

- After the agent is installed, you can enable protection for the servers.
- Before enabling HSS, you need to allocate a quota to a specified server. If the service is disabled or the server is deleted, the quota can be allocated to other servers.

Step 5 **View detection results** and handle risks.

----End

1.6 Can HSS Protect Local IDC Servers?

Yes, as long as your servers connect to the Internet.

1.7 Is HSS in Conflict with Any Other Security Software?

HSS may conflict with DenyHosts, G01, or 360 Guard (server edition).

Conflicts Between the Agent and DenyHosts

For details, see **Is the Agent in Conflict with Any Other Security Software?**

Conflicts Between the Two-factor Authentication Function and G01 or 360 Guard (Server Edition)

On a Windows server where HSS is enabled, the two-factor authentication function may conflict with the login authentication function of G01 or 360 Guard (server edition). In this case, enable only one of the functions as needed.

1.8 What Are the Differences Between HSS and WAF?

HSS and Web Application Firewall (WAF) are provided by Huawei Cloud to help you defend servers, websites, and web applications against risks and threats, improving system security. It is recommended that the services be used together.

Table 1-3 Differences Between HSS and WAF

Service Name	Category	Protected Object	Function
HSS (HSS)	Infrastructure security	Servers	• Asset management • Vulnerability management • Detection & Response • Baseline inspection • Web tamper protection
WAF	Application security	Web applications	• Basic web protection • CC attack protection • Accurate access protection

1.9 Can HSS Be Used Across Accounts?

No. Each account must separately purchase and deploy HSS. However, HSS can be shared by multiple IAM users.

Sharing HSS Among Multiple IAM Users

Assume that you have created an account, *domain1*, by registering with Huawei Cloud, and used *domain1* to create two IAM users, *sub-user1a* and *sub-user1b*, in IAM. If you have granted the HSS permissions to *sub-user1b*, *sub-user1b* can then use the HSS service of *sub-user1a*.

1.10 What Is the HSS Agent?

The HSS agent is used to scan all servers and containers, monitor their status in real time, and collect their information and report to the cloud protection center.

There are different agent versions for Linux and Windows OSs. The HSS protection functions will be available after you **install the agent** and enable **HSS protection**.

Functions of the Agent

- The agent runs scan tasks every day in the early morning to scan all servers and containers, monitors their security, and reports information collected from them to the cloud protection center.
- The agent blocks attacks targeted at servers and containers based on the security policies you configured.

NOTE

- If no agent is installed or the agent installed is abnormal, the HSS is unavailable.
- The agent can be installed on Huawei Cloud Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), on-premises IDC servers, and third-party cloud servers.

Linux Agent Processes

The agent process needs to be run by the **root** user.

The agent contains the following processes:

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 Agent Processes

The agent process needs to be run by the **system** user.

The agent contains the following processes:

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

Agent Process Name	Function	Path
upgrade.exe	Upgrades the agent.	C:\Program Files\HostGuard \upgrade.exe

1.11 Can HSS Be Used Across Clouds?

Yes.

If your services are not deployed on Cloud, you can use HSS. HSS can protect Huawei Cloud ECS servers, Huawei Cloud BMS servers, third-party cloud servers, and on-premises IDC servers, helping you centrally manage diversified servers deployed in the same region.

1.12 Can I Upgrade My HSS Edition?

Yes.

Precautions

- The WTP and container editions are the highest editions and cannot be upgraded.
- An edition can be directly upgraded to the enterprise or premium edition. To upgrade to the WTP edition, you need to purchase it separately, and then bind it to a server.
- The basic edition can be upgraded to the enterprise, premium, or WTP edition. The enterprise edition can be upgraded to the premium or WTP edition. The premium edition can be upgraded to the WTP edition only.

Upgrading to the Enterprise/Premium Edition

To upgrade a quota, its **Usage Status** must be **Idle**.

- **Upgrading an idle quota**

  Upgrade the quota on the **Quotas** tab of the **Servers & Quota** page.
- **Upgrading a quota in use**

  a. Unbind the quota from the server it protects.

  b. Check the quota status. It is expected to change to **Idle**.

  c. Upgrade the quota.

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.

1. Purchase WTP on the HSS console.

2. Unbind a server from its existing quota.
3. Bind the server to WTP.

1.13 Can HSS Automatically Detect and Remove Viruses?

HSS can detect intrusion threats, such as malicious programs and ransomware.

- HSS allows you to manually isolate and kill malicious processes and abnormal process behaviors. For details, see **Handling Server Alarms**
- HSS helps you cope with ransomware attacks before, during, and after an intrusion. For details, see **What Is Ransomware?**

You can also install antivirus software to further harden server security.

2 Agent

2.1 Is the Agent in Conflict with Any Other Security Software?

Yes, it may be in conflict with DenyHosts.

- Symptom: The IP address of the login server is identified as an attack IP address and blocked by HSS. After the IP address is unblocked, it still cannot be used for login.
- Cause: HSS and DenyHosts both block possible attack IP addresses, but HSS can not unblock the IP addresses that were blocked by DenyHosts.
- Handling method: Stop DenyHosts.
- Procedure
  a. Log in to the server as the **root** user.
  b. Run the following command to check whether DenyHosts has been installed:

     ps -ef | grep denyhosts.py

     If information similar to the following is displayed, DenyHosts has been installed:

     ```
     [root@hss-test ~]# ps -ef | grep denyhosts.py
     root      64498      1  0 17:48 ?        00:00:00 python denyhosts.py --daemon
     ```

  c. Run the following command to stop DenyHosts:

     kill -9 'cat /var/lock/denyhosts'

  d. Run the following command to cancel the automatic start of DenyHosts upon host startup:

     chkconfig --del denyhosts;

2.2 How Do I Uninstall the Agent?

Two uninstallation methods are available: one-click uninstallation and manual local uninstallation.

Scenario

- The agent was installed using an incorrect package and you need to uninstall it.
- The agent was installed using incorrect commands and you need to uninstall it.
- If the agent fails to be upgraded, uninstall the agent.

Prerequisites

When you uninstall the agent on the management console, the **Agent Status** of the server is **Online**.

Uninstalling the Agent on the Console in One-Click

You can uninstall an HSS agent from the HSS console.

NOTE

After the agent is uninstalled from a server, HSS will not provide any protection for the 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 **Installation & Configuration** > **Server Install & Config**.

Step 4 In the **Operation** column of the target server, click **Uninstall Agent**.

If you need to uninstall agents in batches, you can select servers and click **Uninstall Agent** above the list.

Step 5 In the displayed dialog box, click **OK**.

In the server list, if **Agent Status** of the server is **Not installed**, its agent is successfully uninstalled.

----End

Uninstalling the Agent from the Server

You can manually uninstall an agent on a server when you no longer use HSS or need to reinstall the agent.

NOTE

After the agent is uninstalled from the target server, HSS will not provide any protection for the server.

- **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. Perform the following operations to stop HSS:

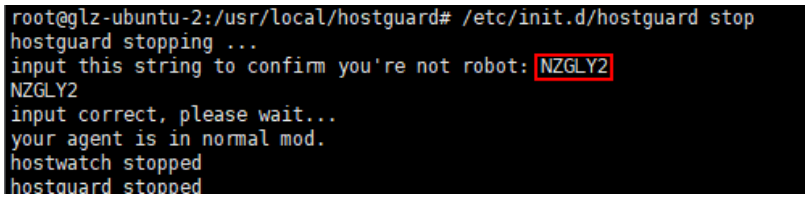
i. Run the following command to stop the service:

/etc/init.d/hostguard stop

ii. (Optional) Enter the verification code displayed in the command output. See **Figure 2-1**.

This operation is required only for servers where HSS self-protection is enabled.

Figure 2-1 Verification code



c. 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.
```

d. (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 stop 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 stop 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. (Optional) Disable HSS self-protection.

If HSS self-protection is enabled, disable it and then uninstall the agent. Otherwise, the agent cannot be uninstalled locally on the server. For details about how to disable the function, see **How Do I Disable Self-Protection?**

b. Log in to the server that you want to uninstall the agent.

c. 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.

d. In the **Uninstall HostGuard** dialog box, click **Yes**.

e. (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.

2.3 What Should I Do If Agent Installation Failed?

If the agent fails to be installed, rectify the fault by following the instructions provided in this section.

Failed to Install the Agent on the HSS Console

If the agent fails to be installed on the console, rectify the fault based on the information displayed on the HSS management console and **Table 2-1**.

Table 2-1 Suggestions for troubleshooting agent Installation failures

Console Message	Suggestion
Connection timed out. Network error.	• Linux Check the network configuration to ensure that the server can access the network. • Windows 1. Run PowerShell as a Windows system administrator. 2. Run the following command to query the service information: **winrm get winrm/config/service** • If the value of **AllowUnencrypted** is **true**, check the network configuration to ensure that the server can access the network. • If the value of **AllowUnencrypted** is **false**, run the following command to change the value to **true**: **winrm set winrm/config/service '@{AllowUnencrypted="true"}'** 3. On the HSS console, install the agent on the Windows server again. 4. After the agent is installed, run the following command to change the value of **AllowUnencrypted** to **false**: **winrm set winrm/config/service '@{AllowUnencrypted="false"}'**
Authentication failed due to incorrect password.	Incorrect password. Please check the password you entered.
The memory space is insufficient.	When installing the agent, ensure that at least 50 MB memory is available. Check and free up memory.
Invalid metadata.	Failed to obtain the metadata. For details, see **Why Can't My Linux ECS Obtain Metadata?**

Console Message	Suggestion
Failed to install expect.	Check whether the network fluctuates. After the network recovers, install the agent again. If the network is normal but the installation still fails, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support.
Failed to connect to VPC.	HSS does not have the VPCOperatePolicy permission. HSS cannot communicate with each other between VPCs. You are advised to perform the following operations to grant the permission: 1. Log in to the HSS console. 2. Click  in the upper left corner and select a region and a project. 3. In the navigation pane, choose **Installation & Configuration** > **Permissions Management**. 4. Click **Assign** in the upper left corner of the permission list to grant the VPCOperatePolicy permission to HSS.
Abnormal DEW key status.	Check and restore your DEW key pair to the normal state.
Failed to connect to VPCEP.	HSS does not have the VPCEPOperatePolicy permission. HSS cannot create a VPC endpoint. The VPC endpoint is used for communication between the agent and the HSS server. You are advised to perform the following operations to grant the permission: 1. Log in to the HSS console. 2. Click  in the upper left corner and select the desired region and project. 3. In the navigation pane, choose **Installation & Configuration** > **Permissions Management**. 4. Click **Assign** in the upper left corner of the permission list to grant the VPCEPOperatePolicy permission to HSS. For details about the meanings and functions of the VPCEPOperatePolicy permission, see .
Failed to log in using the key.	Incorrect password. Please check the password you entered.

Console Message	Suggestion
Insufficient permissions to run the installation command.	Possible cause: The script cannot be executed in the **/tmp** directory, or bash does not have the execution permission. Suggestion: • You are advised to check whether the preceding directories or files have the corresponding permissions. • If the permissions have been granted but the installation still fails, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support.

Console Message	Suggestion
Failed to download the installation file.	This error occurs only on Linux servers. You are advised to perform the following operations to check the security group and DNS configurations. • Checking the security group Log in to the server and run the following command to check whether port 10180 of the 100.125.0.0/16 CIDR block is allowed in the outbound direction of the server security group: **curl -kv https://hss-agent.*region code*.myhuaweicloud.com:10180** Each region has a unique region code. For details about the region code, see **Regions and Endpoints**. Take **CN North-Beijing1** as an example. The complete command is as follows: **curl -kv https://hss-agent.cn-north-1.myhuaweicloud.com:10180** – If the ping command is successfully executed, port 10180 of 100.125.0.0/16 CIDR block has been enabled. – If the page is suspended after the ping command is executed, the port **10180** in the **100.125.0.0/16** network segment is not allowed. For details about how to allow the port, see **Adding a Security Group Rule**. • Checking DNS configurations Log in to the server and run the following command to check whether the DNS of the server can resolve the domain name for downloading the agent: **ping -c 1 hss-agent.*RegionCode*.myhuaweicloud.com** Each region has a unique region code. For details about the region code, see **Regions and Endpoints**. Take **CN North-Beijing1** as an example. The complete command is as follows: ping -c 1 hss-agent.cn-north-1.myhuaweicloud.com – If the resolved IP address is displayed, the DNS resolution is normal. – If **name or service not known** is displayed or no IP address is resolved, the DNS resolution fails. For details, see **Modifying the DNS**.

Console Message	Suggestion
Insufficient disk space.	Check the following directories to ensure that the disk capacity is sufficient: ● Linux – **/usr/local**: default installation path of the agent. Ensure the available disk space is greater than 300 MB. – **/temp**: path for downloading the agent installation package. Ensure the available disk space is greater than 100 MB. ● Windows – **C:\Users\xxx\Downloads**: path for downloading the agent installation package. Ensure the available disk space is greater than 100 MB. – **C:\Program Files\HostGuard**: default installation path of the agent. Ensure the available disk space is greater than 300 MB.
There are no private keys managed by DEW.	Check and ensure that your DEW key pair has been managed.
Installation error.	Perform the following operations: 1. Log in to the HSS console. 2. Click  in the upper left corner and select the desired region and project. 3. In the navigation pane, choose **Installation & Configuration** > **Permissions Management**. 4. Check whether the VPCEPOperatePolicy and VPCOperatePolicy permissions are in the permission list. ● If yes, in the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** and submit a service ticket. ● If no, click **Assign** in the upper left corner of the permission list and grant the VPCEPOperatePolicy and VPCOperatePolicy permissions to HSS. Install the agent again.
The VPC network cannot be connected due to NIC route conflicts.	A route conflict occurs between the NIC of your server and the elastic NIC attached to the server where the agent is being installed. The VPC network cannot be connected. You are advised to install the agent using commands.

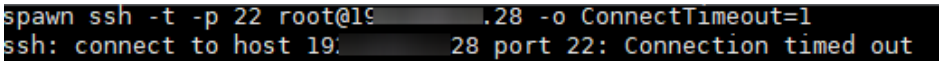
Failed to Install the Agent Using Commands

If you fail to install the agent using commands (that is, by logging in to the server and running commands), rectify the fault based on the command output.

Failed to Install the Agent in Linux

- **Symptom: Connection timed out. Network error.**

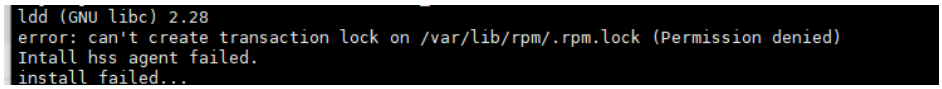
  Figure 2-2 Connection timed out. Network error

  Suggestion: Check the network configuration to ensure that the server can access the network.

- **Symptom: Permission denied.**

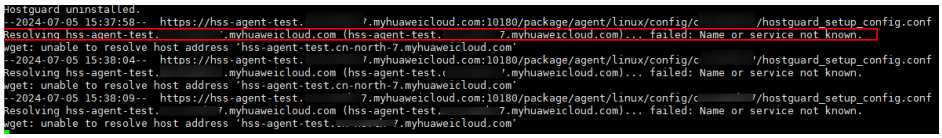
  Figure 2-3 Permission denied

  Suggestion: Log in to the server as the **root** user and run the installation command.

- **Symptom: The domain name cannot be resolved.**

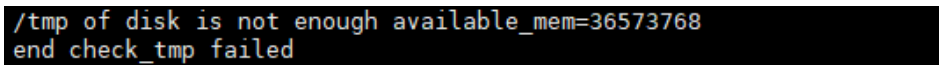
  Figure 2-4 Domain name cannot be resolved

  Suggestion: The server cannot access the agent download address. You need to configure the private DNS address of Huawei Cloud. For details, see **Modifying the DNS**.

- **Symptom: The available disk space of /tmp is less than 100 MB.**

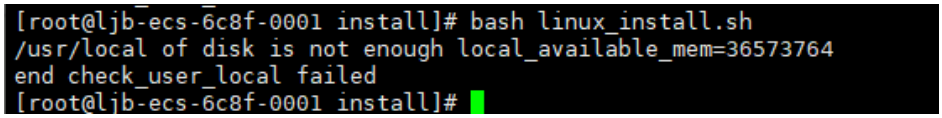
  Figure 2-5 Available disk space of /tmp is less than 100 MB

  Suggestion: The **/tmp** directory is the download path of the agent installation package. Ensure its available disk space is greater than 100 MB.

- **Symptom: The available disk space of /usr/local is less than 300 MB.**

  Figure 2-6 Available disk space of /usr/local is less than 300 MB

Suggestion: The **/usr/local** directory is the default installation directory of the agent. Ensure its available disk space is greater than 300 MB.

- **Symptom: The TLS protocol is incompatible: curl: (35) SSL connect error.**

  Suggestion: Install the HSS agent. The TLS version must be 1.2 or later. If the TLS version does not meet the requirements, manually replace **curl -k -O** in the installation command with **curl --tlsv1.2 -k -O** and install the agent again.

  The following is just an example of command modification. Do not use it directly.

  - Installation command before modification

    curl -k -O 'https://hss-agent.xxx.myhuaweicloud.com:10180/package/agent/linux/install/agent_Install.sh' && echo 'MASTER_IP=hss-agent.xxx.myhuaweicloud.com:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=hss-agent-slave.xxx.myhuaweicloud.com:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=' >> hostguard_setup_config.conf && bash agent_Install.sh && rm -f agent_Install.sh

  - Installation command after modification

    curl --tlsv1.2 -k -O 'https://hss-agent.xxx.myhuaweicloud.com:10180/package/agent/linux/install/agent_Install.sh' && echo 'MASTER_IP=hss-agent.xxx.myhuaweicloud.com:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=hss-agent-slave.xxx.myhuaweicloud.com:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=' >> hostguard_setup_config.conf && bash agent_Install.sh && rm -f agent_Install.sh

Failed to Install the Agent in Windows

If an error message is displayed after you run the script using PowerShell, rectify the fault by referring to the following suggestions:

- **Error message: username and password cannot be empty**

  Suggestion: When you install the agent in batches, the server account or password in the **windows-host-list.xlsx** file you prepared is incorrect. Check and correct it.

- **Error message: remote connect failed**

  Suggestion: To install the agent in batches, the server where the script is executed needs to access the port 5985 on other servers. You need to modify the inbound rules of the security groups on those servers to allow such access. Check whether there are security groups disabling port 5985 in the inbound direction. For details about how to add a security group rule, see **Adding a Security Group Rule**.

- **Error message: download package failed**

  Suggestion: Failed to download the installation package. The server cannot access the agent download address. Check the security group and DNS configurations.

  - Security group: Check whether port 10180 of 100.125.0.0/16 CIDR block is allowed in the outbound direction of the server security group.
  - DNS configurations: Check whether the DNS address of the server is a Huawei Cloud intranet DNS address. For details, see **Modifying the DNS**.

- **Error message: hostguard install failed**

  Suggestion: In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket** and submit a service ticket.

- **Error: Invoke-Command: Failed to perform parameter validation on the session parameter. The parameter is null or empty. Provide a valid parameter and run the command again.**

  Suggestion: Non-encrypted communication is disabled by WinRM service by default. Perform the following operations to allow non-encrypted communication:

  a. Run PowerShell as a Windows system administrator.

  b. Run the following command to check whether HTTP-based WinRM is enabled:

     winrm enumerate winrm/config/listener

     - If error information is returned, WinRM is not enabled. Go to **c**.
     - If no error information is returned, WinRM is enabled. Go to **d**.

  c. Run the following command to enable WinRM and enter **y** to complete the configuration:

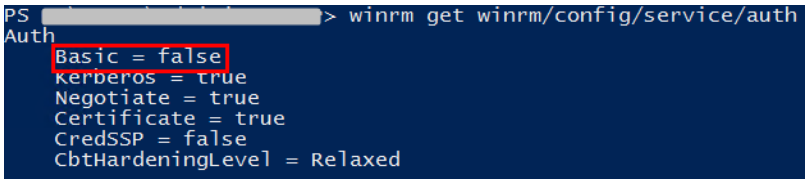
     winrm quickconfig

  d. Configure **Auth**.

     i. Run the following command to view **Auth** information:

     winrm get winrm/config/service/auth

     Figure 2-7 Viewing Auth information

     ii. Run the following command to change the.value of **Basic** to **true**.

     If the value of **Basic** in the command output is **true**, skip this step.

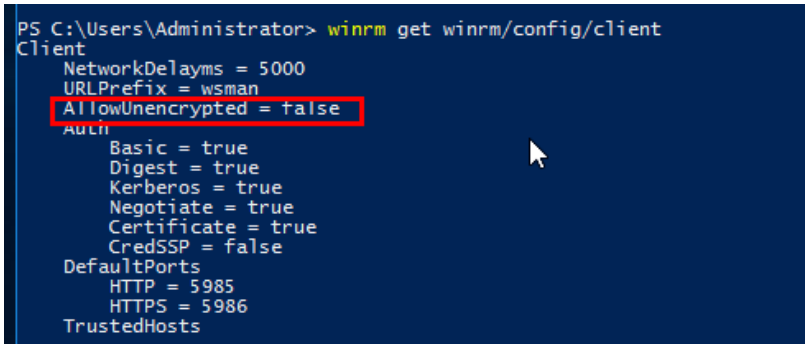
     winrm set winrm/config/service/auth '@{Basic="true"}'

  e. Allow non-encrypted communication.

     i. Run the following command to view client information:

     winrm get winrm/config/client

     Figure 2-8 Viewing client information

If the value of **AllowUnencrypted** is **false** in the command output, go to **e.ii**.

ii. Run the following command to change the value of **AllowUnencrypted** to **true**:

winrm set winrm/config/client '@{AllowUnencrypted="true"}'

2.4 How Do I Fix an Abnormal Agent?

Your agent is probably abnormal if it is in **Not installed** or **Offline** state. Agent statuses and their meaning are as follows:

- **Uninstalled**: No agent has been installed on the server, or the agent has been installed but not started.
- **Offline**: The communication between the agent and the server is abnormal. The agent on the server has been deleted, or a non-Huawei Cloud server is offline.
- **Online**: The agent on the server is running properly.

Possible Causes

- The agent status on the console is not updated.

  The agent status has not been updated. After the agent is installed, it takes 5 to 10 minutes for the console to update its status.
- OS version not supported.

  For details, see "Constraints" in "Service Overview".
- The network is faulty.

  The agent or the cloud protection center is abnormal. For example, the NIC is faulty, the IP address changes, or the bandwidth is low.
- The agent process is abnormal.

Solution

Step 1 Check whether the agent status remains **Offline** on the console for more than 10 minutes after the agent was installed.

- If yes, go to **2**.
- If no, wait until the agent goes online. No further action is required. After the agent was installed, it takes 5 to 10 minutes for the console to update its status.

Step 2 Check whether your server OS is within the scope of support in "Constraints" in "Service Overview".

- If yes, go to **3**.
- If no, the HSS agent cannot be installed or run on your server. Upgrade the OS to a version supported by HSS and try again.

Step 3 Check whether the server network is normal.

- If yes, go to **4**.
- If no, ensure the security group of your server allows access to port 10180 of the 100.125.0.0/16 CIDR block in the outbound direction and the server can

access the network. After the server can access the network, check the agent status.

Step 4 Check whether the available memory of the server is greater than 300 MB.

- If yes, go to **5**.
- If no, the agent will go offline due to insufficient server memory. After the capacity expansion is complete, the agent will go online again.

Step 5 Restart the agent process.

- Windows
  a. Log in to the server as user **administrator**.
  b. Open the Task Manager.
  c. On the **Services** tab page, select **HostGuard**.
  d. Right-click the service and choose **Restart**.
- Linux

  Run the following command in the CLI as user **root** to restart the agent:

  /etc/init.d/hostguard restart

  If the following information is displayed, the restart is successful:

```
root@HSS-Ubuntu32:~#service hostguard restart/etc/init.d/hostguard  restart
Stopping Hostguard...
Hostguard stopped
Hostguard restarting...
Hostguard is running
```

After the process is restarted, wait for about 2 minutes.

- If the agent status is **Online**, no further action is required.
- If the agent status is still **Not installed** or **Offline**, uninstall the agent and install it again.

----End

2.5 What Is the Default Agent Installation Path?

The agent installation paths on servers running the Linux or Windows OS cannot be customized. **Table 2-2** describes the default paths.

Table 2-2 Default agent installation paths

OS	Default Installation Path
Linux	/usr/local/hostguard/
Windows	C:\Program Files\HostGuard

2.6 How Many CPU and Memory Resources Are Occupied by the Agent When It Performs Scans?

HSS uses lightweight agents, which occupy only a few resources and do not affect your services.

The CPU and memory usage is as follows.

Maximum CPU Usage

A running agent occupies a maximum of 20% of a vCPU. The actual usage depends on your server specifications. For details, see **Resource Usage of Different Specifications While the Agent Is Running**.

If the CPU usage exceeds 20% of a vCPU, the agent will automatically reduce CPU usage, spending more time on scans. This does not affect your services. If the CPU usage exceeds 25% of a vCPU, the agent will be automatically restarted.

NOTE

- The agent is scheduled to scan your servers from 00:00 to 04:00 every day. It does not affect the normal running of the server system.
- If an agent is performing a virus scan task, the virus scan program occupies an extra part of the CPU. The CPU usage cannot exceed 30% of the multi-core CPU.

Peak Memory Usage

A running agent occupies about 500 MB memory. If the agent memory usage exceeds the maximum memory limit 500 MB, the agent will be automatically restarted within 5 minutes.

NOTE

If an agent is performing a virus scan task, the average memory usage is 800 MB.

Resource Usage of Different Specifications While the Agent Is Running

The following table describes the CPU and memory usage of different specifications when the agent is running.

Table 2-3 Resource usage of the agent

vCPUs	Max. CPU Usage of Agent	Memory Usage During Virus Scan (Peak Value)	Max. Memory Usage	Memory Usage During Virus Scan (Average Value)
1 vCPU	20%	50%	500MB	800MB
2 vCPUs	10%	40%	500MB	800MB

vCPUs	Max. CPU Usage of Agent	Memory Usage During Virus Scan (Peak Value)	Max. Memory Usage	Memory Usage During Virus Scan (Average Value)
4 vCPUs	5%	35%	500MB	800MB
8 vCPUs	2.5%	32.5%	500MB	800MB
12 vCPUs	About 1.67%	About 31.67%	500MB	800MB
16 vCPUs	About 1.25%	About 31.25%	500MB	800MB
24 vCPUs	About 0.84%	About 30.84%	500MB	800MB
32 vCPUs	About 0.63%	About 30.63%	500MB	800MB
48 vCPUs	About 0.42%	About 30.42%	500MB	800MB
60 vCPUs	About 0.34%	About 30.34%	500MB	800MB
64 vCPUs	About 0.32%	About 30.32%	500MB	800MB

2.7 Do Different HSS Editions Share the Same Agent?

All HSS editions can use the same agent installed on a server.

2.8 How Do I View Servers Where No Agents Have Been Installed?

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** > **Server Install & Config**. The agent management page is displayed.

Step 4 Click the value of **Servers Without Agents** area to filter the servers that have not installed agents.

Possible agent statuses are:

- **Not installed**: The agent has not been installed or successfully started.
- **Installing**: The agent is being installed.

----End

2.9 What Resources Will Be Accessed by the Agent After It Is Installed on a Server?

Table 2-4 describes the devices, IP addresses, and ports that ECSs usually access after the agent is installed.

Table 2-4 IP addresses description

Source Device	Source IP	Source Port	Destination Device	Target IP	Destination Port (Listening)	Protocol	Access Description	Remarks
HSS Agent	Management IP address of the agent	Random	HSS server	HSS server-IP1 HSS server-IP2	10180	TCP	The HSS agent can access HSS server nodes to obtain policies, configurations, and instructions delivered by the server, download agent software packages, upgrade packages, and signature databases, report alarm events, asset fingerprint databases, and baseline check results, and upload suspicious executable program files with user authorization.	The IP address of the HSS server in each region is different. The agent accesses each IP address using a domain name. For details about the domain name of each region, see the installation commands in "Agent Installation Guide".

Source Device	Source IP	Source Port	Destination Device	Target IP	Destination Port (Listening)	Protocol	Access Description	Remarks
			Metadata service node	IP address of the metadata service node	80		The HSS agent obtains the metadata information of the server where the agent is located, including the UUID, availability_zone, project_id, and enterprise_project_id of the ECS.	-

2.10 How Do I Use Images to Install Agents in Batches?

You can use an existing private image to install and deploy an agent on a new server.

NOTE

Do not use existing private images across regions. Otherwise, the agent status will be **Uninstalled**.

For example, if you create a private image in region A and deploy it in region B, after the deployment is complete, the agent status in region B is **Uninstalled**. If you deploy the image in region A, the agent status is **Installed**.

If you need to use an image across regions, install the image, **uninstall the agent in the original region** and clear its information, obtain the agent installation command in the target region, and then run commands to **install the agent** in the target region.

Windows

Perform the following steps to install Windows agents in batches by using images:

Step 1 Purchase a Huawei Cloud ECS. Select the target Windows image. For details, see **Purchasing an ECS**.

Step 2 Install HSS agent on the ECS. For details, see **Installing an Agent**.

NOTE

Do not enable services or modify configurations other than those required for installing HSS agents.

Step 3 Perform the following operations to view the protection status of an ECS:

1. Log in to the console.
2. Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **HSS**.
3. In the navigation pane, choose **Asset Management** > **Servers & Quota**.
4. Click the **Servers** tab.
5. View the protection status in the **Protection Status** column of a server.
   - If the status is **Protected**, go to step **Step 4**.
   - If the status is **Unprotected** or **Protection interrupted**, go to step **Step 5**.

Step 4 Perform the following operations to disable HSS:

1. In the **Operation** column of a server, click **Disable Protection**.
2. Click **OK**.
3. If the **Protection Status** of the server is **Unprotected**, the protection has been disabled.

Step 5 Stop the HostGuard process in the Windows Task Manager.

Step 6 Stop the ECS and use it to create an image. For details, see **Creating an Image**

NOTE

After stopping the ECS, do not restart it before creating an image. Otherwise, you need to repeat **Step 3**.

Step 7 Use the image created in **step 6** to install agents on Windows ECSs in batches.

NOTE

The agent status will be automatically refreshed 5 to 10 minutes after the installation succeeded.

----End

Linux

Perform the following steps to install agents on Linux server in batches by using images:

Step 1 Purchase a Huawei Cloud ECS and select the required Linux image. For details, see **Purchasing an ECS**.

Step 2 Install the agent on the purchased ECS. For details, see **Installing an Agent**.

NOTE

Do not enable services or modify configurations other than those required for installing HSS agents.

Step 3 Perform the following operations to view the protection status of an ECS:

1. Log in to the console.
2. Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **HSS**.
3. In the navigation pane, choose **Asset Management** > **Servers & Quota**.
4. Click the **Servers** tab.
5. View the protection status in the **Protection Status** column of a server.
   - If the status is **Protected**, go to step **Step 4**.
   - If the status is **Unprotected** or **Protection interrupted**, go to step **Step 5**.

Step 4 Perform the following operations to disable HSS:

1. In the **Operation** column of a server, click **Disable Protection**.
2. Click **OK**.
3. If the **Protection Status** of the server is **Unprotected**, the protection has been disabled.

Step 5 Stop the HSS process on the ECS.

Run the **ps -ef** command to check the PID of the HSS, and then run the **kill -pid** command to stop the hostguard process in the Linux OS.

Step 6 Stop the ECS and use it to create an image. For details, see **Creating an Image**.

NOTE

After the ECS is stopped, do not restart it before creating an image. Otherwise, you need to perform steps 3 and 4 again.

Step 7 Use the image created in **step 6** to install agents on Linux ECSs in batches.

NOTE

The agent status will be automatically refreshed 5 to 10 minutes after the installation succeeded.

----End

2.11 What Do I Do If I Cannot Access the Download Link of the Windows Or Linux Agent?

Possible Causes

The link for downloading the agent is a Huawei Cloud private address. Before downloading the agent, you need to configure a Huawei Cloud private DNS address for your server. Otherwise, the server cannot access the link.

Solution

Reconfigure the correct private DNS server address. Resolve the server domain name by using a **private dns server addresses provided by Huawei Cloud** and then open the link for downloading the corresponding agent.

2.12 What Do I Do If Agent Upgrade Fails and the Message "File replacement failed" Is Displayed?

Symptom

On the HSS console, choose **Installation & Configuration** and click the **Agents** tab. After the agent is upgraded, the agent upgrade status is **Upgrade failed**. When you hover your cursor over the status, the message "File replacement failed" is displayed.

Solution

HSS agent 3.2.4 or earlier cannot be directly upgraded to the latest version. You need to manually uninstall the old agent and install the latest HSS agent. For details, see:

1. **Uninstalling the Agent**
2. **Installing an Agent**

3 Vulnerability Management

3.1 How Do I Fix Vulnerabilities?

Procedure

Step 1 Check the vulnerability detection results.

Step 2 Based on provided solutions, fix vulnerabilities one by one in descending order by severity.

- Restart the Windows OS after you fix its vulnerabilities.
- Restart the Linux OS after you fix its kernel vulnerabilities.

Step 3 HSS scans all Linux servers, Windows servers, and Web-CMS servers for vulnerabilities every early morning. After you fix the vulnerabilities, you are advised to perform a check immediately to verify the result.

----End

3.2 What Do I Do If an Alarm Still Exists After I Fixed a Vulnerability?

Perform the following operations to locate the cause and fix the problems.

NOTE

For details about how to fix vulnerabilities, see **Fixing Vulnerabilities and Verifying the Result**.

Possible Causes and Solutions on a Linux Server

- No yum sources have been configured.

  In this case, configure a yum source suitable for your Linux OS, and fix the vulnerability again.
- The yum source does not have the latest upgrade package of the corresponding software.

Switch to the yum source having the required package and fix the vulnerability again.

- The intranet environment cannot connect to Internet.

  Servers need to access the Internet and use external yum sources to fix vulnerabilities. If your servers cannot access the Internet, or the external image sources cannot provide stable services, you can use the image source.

- The old kernel version remains.

  Old kernel versions often remain in servers after upgrade. You can run the **verification commands** to check whether the current kernel version meets the vulnerability fix requirements. If it does, ignore the vulnerability on the **Linux Vulnerabilities** tab of the **Vulnerabilities** page. You are not advised to delete the old kernel.

  Table 3-1 Verification commands

OS	Verification Command
CentOS/Fedora /Euler/Red Hat/Oracle	rpm -qa | grep *Software_name*
Debian/Ubuntu	dpkg -l | grep *Software_name*
Gentoo	emerge --search *Software_name*

- **The server is not restarted after the kernel vulnerability is fixed.**

  After the kernel vulnerability is fixed, restart the server. If the server is not restarted, the vulnerability alarm still exists.

3.3 Why a Server Displayed in Vulnerability Information Does Not Exist?

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.

3.4 Do I Need to Restart a Server After Its Vulnerabilities Are Fixed?

After you fixed Windows OS vulnerabilities or Linux kernel vulnerabilities, you need to restart servers for the fix to take effect, or HSS will continue to warn you of these vulnerabilities. For other types of vulnerabilities, you do not need to restart servers after fixing them.

3.5 Can I Check the Vulnerability and Baseline Fix History on HSS?

Viewing Fixed 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**.

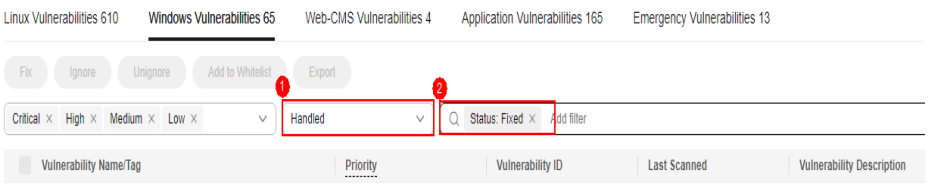
Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 On the vulnerability tabs, filter and view fixed vulnerabilities.

NOTICE

Vulnerabilities are displayed in the vulnerability list only for seven days. You can only check the vulnerabilities that have been fixed in the last seven days.

Figure 3-1 Filtering fixed vulnerabilities



----End

Viewing Fixed Baseline Issues

The fix history does not show the password complexity policy settings or common weak passwords that have been fixed. To check other fixed configuration items, perform 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 In the navigation pane, choose **Risk Management** > **Baseline Checks**.

Step 4 Click the **Unsafe Configurations** tab.

Step 5 Click a baseline name to go to the details page.

Step 6 On the **Check Items** tab, view the check items in **Passed** state.

----End

3.6 What Do I Do If Vulnerability Fix Failed?

If Linux or Windows vulnerabilities failed to be fixed on the HSS console, rectify the fault by following the instructions provided in this section.

Viewing the Cause of a Vulnerability Fixing Failure

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 **Risk Management** > **Vulnerabilities**.

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 **Vulnerabilities** page, click **Manage Task**.

Step 5 Click the **Fix Tasks** tab to view the vulnerability fixing results.

- : The number displayed next to this icon indicates the number of servers that are successfully fixed.
- : The number displayed next to this icon indicates the number of servers that failed to be fixed.

Step 6 Click . In the **Fix Failures** dialog box, view the failure cause and description.

You can handle the vulnerability fixing failures based on the failure causes. For details, see **Linux Vulnerability Fixing Failure Causes and Solutions** and **Windows Vulnerability Fixing Failure Causes and Solutions**.

----End

Linux Vulnerability Fixing Failure Causes and Solutions

NOTICE

- The kernel vulnerabilities on CCE, MRS, and BMS servers cannot be fixed. Fixing them may make some functions unavailable.
- After the kernel vulnerability is fixed, you need to restart the server. If you do not restart the server, the vulnerability alarm still exists.
- The following failure causes only contain some key fields. For details, see the information displayed on the HSS console.

Failure Cause	Description	Solution
timeout	Repair timed out.	Wait for 1 hour and try fixing the vulnerability again. If the fault persists, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support.
This agent version does not support vulnerability verification	The agent version is too early.	**Upgrade the agent** and try fixing the vulnerability again.
Agent status is not normal	The agent status is abnormal.	The agent is offline and the vulnerability cannot be fixed. Recover the agent status by referring to **How Do I Fix an Abnormal Agent?** and fix the vulnerability.

Error: software have multiple versions	A software version with vulnerabilities is not deleted.	• If this problem occurs in common software, delete the packages of the earlier versions and check whether the problem persists.
		Run the following command to check whether an error is reported when an early version package is deleted:
		`rpm -e --test XXX`
		NOTE
		XXX indicates the full software component name, which contains the version number. You can run the **rpm -qa** command to query the full component name.
		– If an error is reported during the deletion, there are dependencies on the software package, and the package cannot be deleted. You are advised to ignore this vulnerability.
		– If no error is reported during the deletion, run the following command to delete the early version package:
		`rpm -e XXX`
		• If this problem occurs on kernel-related components such as Kernel and Glibc, deleting the early version package may cause OS problems. In this case, you are advised to ignore this vulnerability.

Failure Cause	Description	Solution
No package marked for update Error: software info not update Error: kernel is not update is already the newest version Dependencies resolved. Nothing to do. Complete!	The upgrade package of a later version is not found.	The failure cause indicates that the software has been upgraded to the latest version supported by the current image source, but the vulnerability still exists. **NOTE** • CentOS 7, CentOS 8, Debian 9 and 10, Windows 2012 R2, and Ubuntu 14.04 and earlier have reached EOL and cannot be fixed because no official patches are available. You are advised to change to the OSs in active support. • Ubuntu 15.04 to Ubuntu 22.04 do not support free patch updates. You need to subscribe to Ubuntu Pro to install upgrade packages. If Ubuntu Pro is not configured, vulnerabilities will fail to be fixed. • Possible cause 1: The image source is incorrectly configured. Update the image source and fix the vulnerability again. For more information, see "Image Source Management". • Possible cause 2: Kernel vulnerabilities cannot be fixed on the server. Fixing kernel vulnerabilities may make some functions unavailable. To fix a kernel vulnerability, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support. **NOTICE** The kernel vulnerabilities on CCE, MRS, and BMS servers cannot be fixed. Fixing them may make some functions unavailable. Do not upgrade kernel components.
Error: Failed to download metadata for repo One of the configured repositories failed Errors during downloading metadata for repository Error: Cannot retrieve repository metadata Failed connect to	Failed to connect to the yum source.	The server cannot connect to the image source. Check whether the server can properly connect to the external network.

Failure Cause	Description	Solution
E: Failed to fetch		
Error: kernel is not update Error: kernel info not update	Kernel not updated.	• Possible cause 1: The server is not restarted after the vulnerability is fixed. Solution: Restart the server. After a kernel vulnerability is fixed, you need to restart the server for the fix to take effect. Otherwise, the system will still report the vulnerability in the next scan. • Possible cause 2: Kernel vulnerabilities cannot be fixed on the server. Fixing kernel vulnerabilities may make some functions unavailable. To fix a kernel vulnerability, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support.
Please install a package which provides this module, or verify that the module is installed correctly command not found	The yum command is unavailable.	Rectify the command unavailability issue based on the suggestions provided in the failure cause.
Error downloading packages	The upgrade package fails to be downloaded.	Check whether the server can properly connect to the Internet. • If yes, the image source is incorrectly configured. Update the image source and fix the vulnerability again. • If no, ensure that your server can connect to the Internet and fix the vulnerability again.
There are no enabled repositories Error: Cannot find a valid baseurl for repo There are no enabled repos	No available sources configured.	This fault occurs because the image source is incorrectly configured. Update the image source and fix the vulnerability again.

Failure Cause	Description	Solution
dpkg was interrupted	The dpkg command is unavailable.	Rectify the command unavailability issue based on the suggestions provided in the failure cause.

Windows Vulnerability Fixing Failure Causes and Solutions

NOTICE

- After a Windows patch is installed, you need to restart the server, or the following problems may occur:
  - The patch does not take effect.
  - When you install other system patches or software, the blue screen of death (BSOD) or startup failure may occur.
- The following failure causes only contain some key fields. For details, see the information displayed on the HSS console.

Failure Cause	Description	Solution
timeout	Repair timed out.	Wait for 1 hour and try fixing the vulnerability again. If the fault persists, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support.
Agent status is not normal	The agent status is abnormal.	The agent is offline and the vulnerability cannot be fixed. Recover the agent status by referring to **How Do I Fix an Abnormal Agent?** and fix the vulnerability.
This agent version does not support vulnerability verification	The agent version is too early.	**Upgrade the agent** and try fixing the vulnerability again.

Failure Cause	Description	Solution

Search patch failed: Search failed, errmsg(Unknown error 0x8024401C)	Failed to find the patch.	The fault occurs because the Windows Update component on the server is faulty. Perform the following operations to recover the Windows Update component and fix the vulnerability again:
		1. Open the command-line interface (CLI).
		2. Run the following commands one by one:
		`net stop wuauserv`
		`reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
		`net start wuauserv`

Search patch failed: Search failed, errmsg(Unknown error 0x8024402C)	Failed to find the patch.	The fault occurs because the Windows Update client cannot connect to the Windows Update server. Perform the following operations to recover the Windows Update component and fix the vulnerability again:
		1. Check whether the network connection of the server is normal.
		Ensure your server can connect to the Internet.
		2. Clear the Windows Update cache.
		a. Open **Control Panel**.
		b. Click **System and Security**. Under **Administrative Tools**, click **Services**.
		c. Right-click **Windows Update** and choose **Stop**.
		d. Open the **C:\Windows** folder. Delete the **SoftwareDistribution** file.
		e. Right-click the **Windows Update** service and choose **Start**.
		3. Run the following commands to reset the Windows Update component:
		`net stop wuauserv`
		`net stop cryptSvc`
		`net stop bits`
		`net stop msiserver`
		`ren C:\Windows\SoftwareDistribution SoftwareDistribution.old`
		`ren C:\Windows\System32\catroot2 catroot2.old`
		`net start wuauserv`
		`net start cryptSvc`
		`net start bits`
		`net start msiserver`

<table>
<tr><th>Failure Cause</th><th>Description</th><th>Solution</th></tr>
<tr><td>Search patch failed: Search failed, errmsg(Unknown error 0x80070422)</td><td>Failed to find the patch.</td><td>The fault occurs because Windows Update is disabled on the server. Perform the following operations to start the service and fix the vulnerability again:
1. Open Control Panel.
2. Click System and Security. Under Administrative Tools, click Services.
3. Double-click the Windows Update service.
4. In the Windows Update Properties window, set Startup type to Automatic.
5. Click OK.</td></tr>
<tr><td>Search patch failed: Get updates count is 0</td><td>Failed to find the patch.</td><td rowspan="8">The fault occurs because the Windows Update of the server is faulty. Perform the following steps to locate the fault:
1. Check whether the network connection of the server is normal.
• If yes, go to 2.
• If no, fix the vulnerability again after the server network connection becomes normal.
2. Open Windows Update and check whether the patch to be installed is available.
• If yes, install the patch and restart the server.
• If no, check whether the failure cause contains an error code.
If it contains an error code, search for the corresponding solution on the Microsoft official website based on the error code.
If it does not contain any error code, reset Windows Update by referring to Reset Windows Update.</td></tr>
<tr><td>Search patch failed: Search failed,errmsg</td><td>Failed to find the patch.</td></tr>
<tr><td>Not install security patch</td><td>Failed to find the patch.</td></tr>
<tr><td>Add patch to update collection failed: Update collection count is 0</td><td>Failed to find the patch.</td></tr>
<tr><td>Not find patch</td><td>No patches found.</td></tr>
<tr><td>Add patch to update collection failed</td><td>Failed to install the patch.</td></tr>
<tr><td>Com init failed</td><td>Failed to call Windows Update.</td></tr>
</table>

Failure Cause	Description	Solution
Download patch failed	Failed to download the patch.	• Possible cause 1: The Windows Update configuration is incorrect. This problem may occur only in Windows 2008 and 2012. Open **Control Panel**. Click **Windows Update** and click **Change settings**. Configure the following parameters: – **Important updates**: Select **Download updates but let me choose when to install them**. – **Recommended update**: Select this check box. – **Microsoft Update**: Deselect this check box. After the configuration is complete, open Windows Update and click **Check for Update**. After the patches to be installed are found, install them and restart the server. • Possible cause 2: The server has not been patched for a long time. As a result, Windows Update is abnormal. 1. Log in to the server and open Windows Update. 2. Click **Check for Update**. 3. After the patches to be installed are found, install them and restart the server. **NOTE** Some patches probably cannot be installed at a time. Check for updates after every patch installation until all patches are installed.

3.7 Why Can't I Select a Server During Manual Vulnerability Scanning or Batch Vulnerability Fixing?

Possible Causes

During manual vulnerability scanning or batch vulnerability fixing, the following servers cannot be selected:

- Servers that are not in the **Running** state
- Servers whose agent status is **Offline**

Solution

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**.

Step 4 On the **Servers** tab, view the server running status, agent status, and HSS version.

Figure 3-2 Viewing server information

Confirm related information and perform the following operations to rectify the fault:

- Servers are protected by basic edition HSS.

  The HSS basic edition does not support manual vulnerability scan and batch vulnerability fixing. To use these features, upgrade the HSS edition. For details, see **Upgrading Your Edition**.
- Servers that are not in the **Running** state

  Check the server and ensure the server status is **Running**.
- Servers whose agent status is **Offline**

  An offline agent cannot receive instructions delivered from the console. To put the agent back online, perform the operations described in **How Do I Fix an Abnormal Agent?**

Step 5 In the navigation pane, choose **Risk Management** > **Vulnerabilities**. Select the servers you want to manually scan or fix in batches again. If the target server can be selected, the problem has been fixed.

----End

3.8 What Do I Do If a Vulnerability Scan Fails?

If a vulnerability scan fails on the HSS console, rectify the fault by following the instructions provided in this section.

Viewing the Cause of a Vulnerability Scan Failure

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 **Risk Management** > **Vulnerabilities**.

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 **Vulnerabilities** page, click **Manage Task**.

Step 5 Click the **Scan Tasks** tab to view vulnerability scan results.

- : The number displayed next to this icon indicates the number of servers that are successfully scanned.
- : The number displayed next to this icon indicates the number of servers that failed to be scanned.

Step 6 Click the icon. In the **Scan Failures** dialog box, view the server information and the failure cause.

You can handle the vulnerability scan failure based on the failure cause. For details, see **Vulnerability Scan Failure Causes and Solutions**.

----End

Vulnerability Scan Failure Causes and Solutions

Table 3-2 Vulnerability scan failure causes and solutions

Failure Cause	Solution
Scan timed out. Agent is in silent or no-load mode.	Perform the following operations to restart the agent and scan for vulnerabilities again: • Windows 1. Log in to the server as user **administrator**. 2. Open the Task Manager. 3. On the **Services** tab page, select **HostGuard**. 4. Right-click the service and choose **Restart**. • Linux Run the following command in the CLI as user **root** to restart the agent: **/etc/init.d/hostguard restart** If the following information is displayed, the restart is successful: root@HSS-Ubuntu32:~#service hostguard restart/etc/init.d/hostguard restart Stopping Hostguard... Hostguard stopped Hostguard restarting... Hostguard is running If the scan still fails, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support.
The agent version is too early.	**Upgrade the agent** to the latest version and scan for vulnerabilities again.

Failure Cause	Solution
Asset discovery policy disabled.	Choose **Security Operations** > **Policies**, select the policy group that the server belongs to, and check whether the **Asset Discovery** policy is enabled. If the policy is not enabled, enable it, wait for 10 minutes, and scan for vulnerabilities again. If the policy is enabled but the scan still fails, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support.
Failed to execute some detection scripts.	Choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support.
Failed to deliver the scan command.	Try scanning for vulnerabilities again. If the scan still fails after multiple attempts, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the Huawei Cloud management console to contact technical support.
The scan command was lost.	
Failed to obtain agent information.	
Failed to detect vulnerabilities.	
Failed to update vulnerability data.	
Failed to update part of vulnerability data.	
Failed to load the vulnerability database.	
The agent did not report the file list.	
Failed to obtain the vulnerability scan status.	

4 Detection & Response

4.1 How Do I View and Handle HSS Alarm Notifications?

Viewing Alarms

For details about how to view HSS alarms, see **Viewing Intrusion Alarms**. For details about how to view CGS alarms, see **Viewing Container Alarms**.

Handling Alarms

You can fix vulnerabilities, check and block intrusions, and fix unsafe settings based on suggestions provided. For details, see **Handling Server Alarms**.

For details about how to handle container alarms, see **Handling Container Alarms**.

4.2 What Do I Do If My Servers Are Subjected to a Mining Attack?

Take immediate measures to contain the attack, preventing miners from occupying CPU or affecting other applications. If a server is intruded by a mining program, the mining program may penetrate the intranet and persist on the intruded server.

You should also harden your servers to better block intrusions.

Troubleshooting Procedure

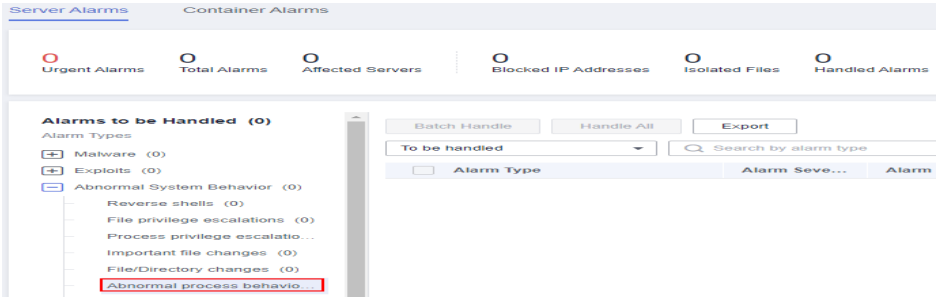
Step 1 Log in to the management console.

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

Step 3 Check **Abnormal process behavior** events.

Choose **Detection & Response** > **Alarms** and click **Server Alarms**. Choose **Abnormal System Behavior** > **Abnormal process behavior** to view and handle the abnormal process behavior alarms. Click **Handle** in the **Operation** column of an event.

Figure 4-1 Handling abnormal process behavior



Step 4 Check auto-startup items. Some of your auto-startup items were probably created by attackers to start mining programs upon server restart.

Choose **Asset Management** > **Server Fingerprints**, click **Auto-startup**, and select **Operation History** to view the change history.

----End

Hardening Servers

After you delete miner programs, harden your servers to better defend against intrusions.

Linux servers

1. Let HSS automatically scan your servers and applications in the early morning every day to help you detect and eliminate security risks.
2. Set stronger passwords for all accounts (including system and application accounts), or change the login mode to key-based login.
   a. Set the security password. For details, see **How Do I Set a Secure Password?**.
   b. Use the key to log in to the server. For details, see **Using a Private Key to Log In to the Linux ECS**.
3. Strictly control the usage of system administrator accounts. Grant only the least permissions required for applications and middleware and strictly control their usage.
4. Configure access rules in security groups. Open only necessary ports. For special ports (such as remote login ports), only allow access from specified IP addresses or use VPN or bastion hosts to establish your own communications channels. For details, see **Security Group Rules**.

Windows servers

Use HSS to comprehensively check for and eliminate security risks. Improve your account, password, and authorization security.

- **Account hardening**

Measure	Description	Procedure
Ensure default account security.	• Disable user **Guest**. • Disable and delete unnecessary accounts. (You are advised to disable inactive accounts for three months before deleting them.)	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Computer Management**. 3. Choose **System Tools** > **Local Users and Groups** > **Users**. 4. Double-click **Guest**. In the **Guest Properties** window, select **Account is disabled**. 5. Click **OK**.
Assign accounts with only necessary permissions to users.	Create users and user groups of specific types. Example: administrators, database users, audit users	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Computer Management**. 3. Choose **System Tools** > **Local Users and Groups**. Create users and groups as needed.
Periodically check and delete unnecessary accounts.	Periodically delete or lock unnecessary accounts.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Computer Management**. 3. Choose **System Tools** > **Local Users and Groups**. 4. Choose **Users** or **User Groups** and delete unnecessary users or user groups.
Do not display the last username.	Forbid the login page from displaying the latest logged in user.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Local Security Policy**. 3. Choose **Local Policies** > **Security Options**. 4. Double-click **Interactive logon: Do not display last user name**. 5. In the displayed dialog box, select **Enable** and click **OK**.

- **Password hardening**

Setting	Description	Procedure
Complexity	In line with the requirements set in **How Do I Set a Secure Password**.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Local Security Policy**. 3. Choose **Account Policies** > **Password Policy**. 4. Enable the policy **Password must meet complexity requirements**.
Maximum password age	In static password authentication mode, force users to change their passwords every 90 days or at shorter intervals.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Local Security Policy**. 3. Choose **Account Policies** > **Password Policy**. 4. Set **Maximum password age** to 90 days or shorter.
Account lockout policy	In static password authentication mode, lock a user account if authentication for the user fails for 10 consecutive times.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Local Security Policy**. 3. Choose **Account Policies** > **Account Lockout Policy**. 4. Set **Account lockout threshold** to **10** or smaller.

- **Authorization hardening**

Authorization	Description	Procedure
Remote shutdowns	Assign the permission **Force shutdown from a remote system** only to the **Administrators** group.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Local Security Policy**. 3. Choose **Local Policies** > **User Rights Assignment**. 4. Assign the permission **Force shutdown from a remote system** only to the **Administrators** group.
Local shutdown	Assign the permission **Shut down the system** only to the **Administrators** group.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Local Security Policy**. 3. Choose **Local Policies** > **User Rights Assignment**. 4. Assign the permission **Shut down the system** only to the **Administrators** group.

Authorization	Description	Procedure
User rights assignment	Assign the permission **Take ownership of files or other objects** only to the **Administrators** group.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Local Security Policy**. 3. Choose **Local Policies** > **User Rights Assignment**. 4. Assign the permission **Shut down the system** only to the **Administrators** group.
Login	Authorize users to log in to the computer locally.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Local Security Policy**. 3. Choose **Local Policies** > **User Rights Assignment**. 4. Assign the permission **Allow log on locally** to the users you want to authorize.
Access from the network	Allow only the authorized users to access this computer from the network (for example, by network sharing). Access from other terminals are not allowed.	1. Open **Control Panel**. 2. Click **Administrative Tools**. Open **Local Security Policy**. 3. Choose **Local Policies** > **User Rights Assignment**. 4. Assign the permission **Access this computer from the network** to the users you want to authorize.

4.3 Why a Process Is Still Isolated After It Was Whitelisted?

After you add a process to the whitelist, it will no longer trigger certain alarms, but its isolation will not be automatically canceled. If your process is isolated, you need to manually restore it.

Isolating and Killing a Malicious Program

- Choose **Installation & Configuration** and click the **Security Configuration** tab. Click the **Isolation and Killing of Malicious Programs** tab and enable this function.
- Choose **Detection & Response** > **Alarms**. In the **Events** area, manually isolate and kill malicious programs.

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.

Canceling the Isolation of Files

1. Choose **Detection & Response** > **Alarms**. Click the value above **Isolated Files** to view the isolated files.
2. In the row containing the target server, click **Restore** in the **Operation** column. The dialog box is displayed.
3. Click **OK** to restore the isolation file.

   After you cancel isolation, the read/write permissions of files will be restored, but terminated processes will not be automatically started.

4.4 Why an Attack Is Not Detected by HSS?

- Intrusions to your servers before HSS is enabled cannot be detected.
- If you have purchased HSS, remember to enable it to detect intrusions.
- Web attacks cannot be detected, because HSS mainly defends your servers. To protect websites, you can consult the security Solution Architect or use other secure services (such as WAF and Anti-DDoS).

4.5 Can I Unblock an IP Address Blocked by HSS, and How?

Whether you can unblock an IP address depends on why it was blocked. An IP address will be blocked if it is regarded as the source of a brute-force attack, listed in the common IP blacklist, or not in the IP whitelist you set.

Brute-force Attack IP Address

- If a brute force attack is detected, HSS blocks the attack source IP address for 12 hours by default. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.
- If you are sure that a source IP address can be trusted, you can manually unblock it. Choose **Detection & Response** > **Alarms**, click **View Details** under **Blocked IP Addresses**, and unblock the IP address in the displayed slide-out panel.

  If you manually unblocked an IP address, but incorrect password attempts from this IP address exceed the threshold again, this IP address will be blocked again.

IP Address in the Common IP Blacklist

You cannot manually unblock such IP addresses.

IP Address Not in the SSH Login IP Whitelist

If you have configured the **SSH login IP whitelist**, the IP addresses not in the whitelist will be blocked. To unblock an IP address, add it to the whitelist.

4.6 Why a Blocked IP Address Is Automatically Unblocked?

If a blocked IP address does not perform brute-force attacks in the next 12 hours, the IP address will be automatically unblocked.

4.7 How Often Is Malware Scan and Removal?

Detection period: real-time detection

Isolation and killing period:

- If you have enabled automatic isolation and killing, the system will scan and kill viruses in real time.
- If you have not enabled automatic isolation and killing, you need to manually check and handle alarms.

NOTICE

1. HSS can detect malicious programs (through cloud-based antivirus) and abnormal process behaviors in real time, report alarms, and isolate and kill them. For details about the detection capabilities, see "Features".
2. HSS isolation and killing can be automatically or manually performed.
   - For more information about automatic isolation and killing, see "Isolating and Killing Malicious Programs" in "Security Configuration".
   - For more information about manual isolation and killing, see "Isolating and Killing Files" in "Managing Isolated Files".

4.8 What Do I Do If an IP Address Is Blocked by HSS?

Check whether the blocked IP address is a malicious IP address or a normal one.

- If it is normal, add it to the whitelist.
- If it is malicious, no further operations are required.

4.9 How Do I Defend Against Ransomware Attacks?

Generally, ransomware is spread through Trojan implantation, emails, files, vulnerabilities, bundles, and storage media.

To defend against ransomware intrusions, **prevent brute-force attacks** and handle HSS alarms in a timely manner.

.

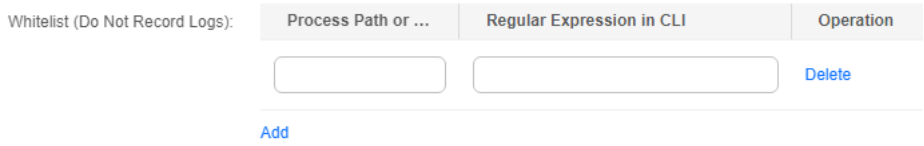
4.10 How Do I Add High-risk Command Execution Alarms to the Whitelist?

If you run commands related to normal services on the server, HSS generates high-risk command execution alarms. You can add a whitelist to prevent the alarm.

To add a command alarm whitelist, perform the following steps:

1. Log in to the management console.
2. In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.
3. In the navigation pane, choose **Security Operations** > **Policies**.
4. Locate the policy group of the protected edition corresponding to the server and click the policy group name.
5. Click **Real-time Process**.
6. Add a command whitelist. The parameters are as follows:
   - Full path or program name of a process: Enter the full path or program name of the process, for example, **/usr/bin/sleep** or **sleep**.
   - Regular expression in CLI: Enter the regular expression of the command to be added to the whitelist, for example, **^[A-Za-z0-9[:space:]*\\.\\ \":_'\\(>=-]+$**.

   Figure 4-2 Adding a whitelist

7. Click **OK** to save the change.

4.11 Why Doesn't HSS Generate Alarms for Some Web Shell Files?

Symptom

HSS does not report alarms for some web shell files.

Possible Causes

The default handle usage of the HSS is 30% of the maximum handles on the server. If the number of user files exceeds the upper limit of the handles scanned by HSS, HSS will be unable to check all the web shell files. As a result, no alarm is reported for unchecked files.

Solution

Step 1 Log in to the server.

Step 2 Create the **check_inotify.sh** file. Copy and save the following content to the file:

```
#!/bin/bash

# Enable the floating-point number comparison mode of Bash.
shopt -s globstar nullglob

# Obtain the value of sysctl fs.inotify.max_user_watches.
max_user_watches=$(sysctl -n fs.inotify.max_user_watches)

# Calculate the value multiplied by 30%.
threshold=$(echo "$max_user_watches * 0.3" | awk '{print int($1)}')

# Calculate the number of files in the /opt/app directory.
app_files_count=$(find /opt/app -type f | wc -l)

# Compare and output the result.
if [[ "$app_files_count" -gt "$threshold" ]]; then
  echo "Current value of fs.inotify.max_user_watches: $max_user_watches"
echo "Number of files in the /opt/app directory: $app_files_count"
  echo "Handle usage problem exists."
else
  echo "Current value of fs.inotify.max_user_watches: $max_user_watches"
echo "Number of files in the /opt/app directory: $app_files_count"
  echo "There are no handle usage problems."
fi
```

Step 3 Run the following command to execute the **check_inotify.sh** file:

chmod +x check_inotify.sh./check_inotify.sh

If the command output shows **Handle usage problem exists**, in the upper right corner of the Huawei Cloud console, choose **Service Tickets** > **Create Service Ticket** and submit a service ticket to contact technical support.

----End

5 Abnormal Logins

5.1 Why Do I Still Receive Remote Login Alarms After Configuring the Login IP Whitelist?

Even whitelisted IP addresses can certain trigger alarms. The SSH login IP address whitelist, Login Whitelist, and remote login functions focus on different aspects of security, as described in **Table 5-1**.

Table 5-1 Functions

Function	Description	How to Mask Alarm
SSH login IP address whitelist	Only the IP addresses in this whitelist can log in to specified servers via SSH. **NOTICE** To avoid connection issues, ensure you have not missed necessary IP addresses before enabling this function.	-
Login Whitelist	To reduce false brute-force attack alarms, add trusted login IP addresses and their destination server IP addresses to the Login Whitelist.	Choose **Detection & Response** > **Whitelists**. Click the **Login Whitelist** tab, and add IP addresses. HSS will not generate brute-force alarms for these IP addresses.
Remote login	Logins not from **Common Login Locations** and **Common Login IP Addresses** will trigger remote login alarms. You will be informed of new IP addresses that log in to your servers.	Choose **Installation & Configuration** and click **Security Configuration**. Add login information on the **Common Login Locations** and **Common Login IP Addresses** tabs. Whitelisted logins will no longer trigger remote alarms.

5.2 How Do I Check the User IP address of a Remote Login?

Alarm Policies

The remote login detection function checks for remote logins into your servers in real time. HSS generates an alarm if it detects logins from locations other than the common login locations you set.

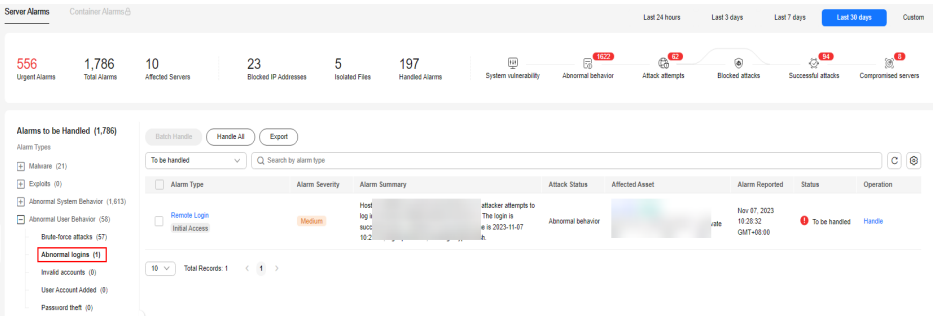
Viewing Remote Login Records on the Console

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 As shown in **Figure 5-1**, check the **Abnormal logins**. Click **Remote Login** and click the alarm name to view details.

Figure 5-1 Abnormal logins



Step 4 In the navigation pane on the left, choose **Detection & Response** > **Alarms**, and click **Server Alarms**.

Step 5 In the **Event Types** area, Choose **Abnormal User Behavior** > **Abnormal logins**, and click **Remote Login**.

----End

Locally Viewing Remote Login Records

- Linux

  For Linux servers, you can view logs in **/var/log/secure** and **/var/log/message** directories, or run the **last** command to check whether there are abnormal login records.

- Windows

  To view server login logs, perform the following steps:

  a. Open **Control Panel**.

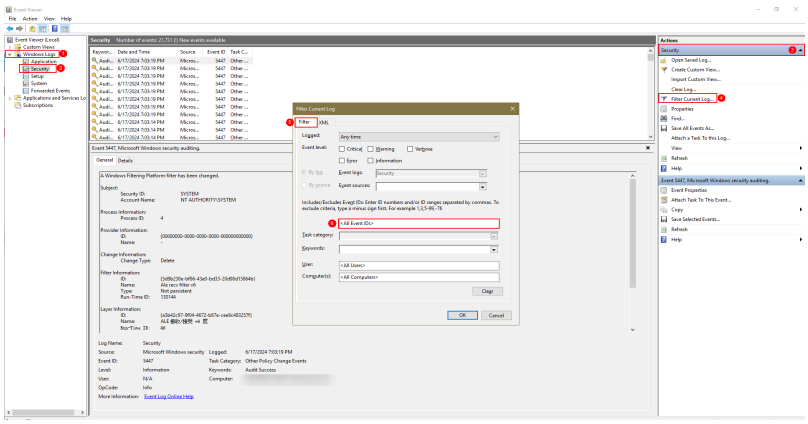
b. Choose **Administrative Tools** > **Event Viewer**. The **Event Viewer** page is displayed.

c. In the navigation tree on the left, choose **Windows Logs** > **Security**. The **Security** page is displayed.

d. In the navigation tree on the right, choose **Security** > **Filter Current Log**. The **Filter Current Log** dialog box is displayed.

e. On the **Filter** tab, locate the **<All Event IDs>**.

Figure 5-2 Filter



f. Enter the login event ID and click **OK** to filter the target login events.

- 4624: ID of successful login events
- 4625: ID of failed login events

5.3 How Do I Cancel the Alarm Notifications of Successful Server Logins?

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

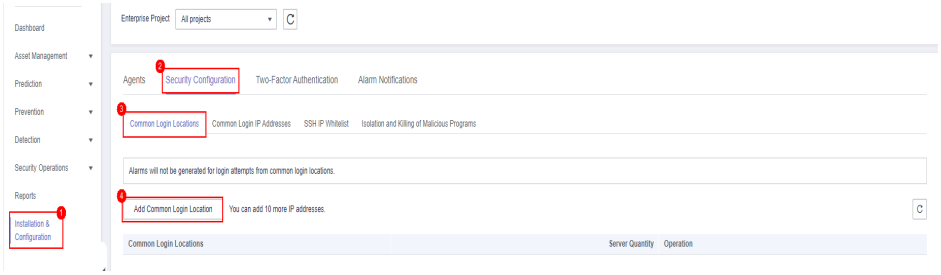
5.4 Can I Disable Remote Login Detection?

No.

If you do not want to receive remote login alarm notifications, add alarmed locations as common login locations, or deselect the remote login attempt item in alarm notification settings.

- On the **Common Login Locations** tab, click **Add Common Login Location**, and add common login locations. HSS does not trigger remote login alarms on logins from common login locations.

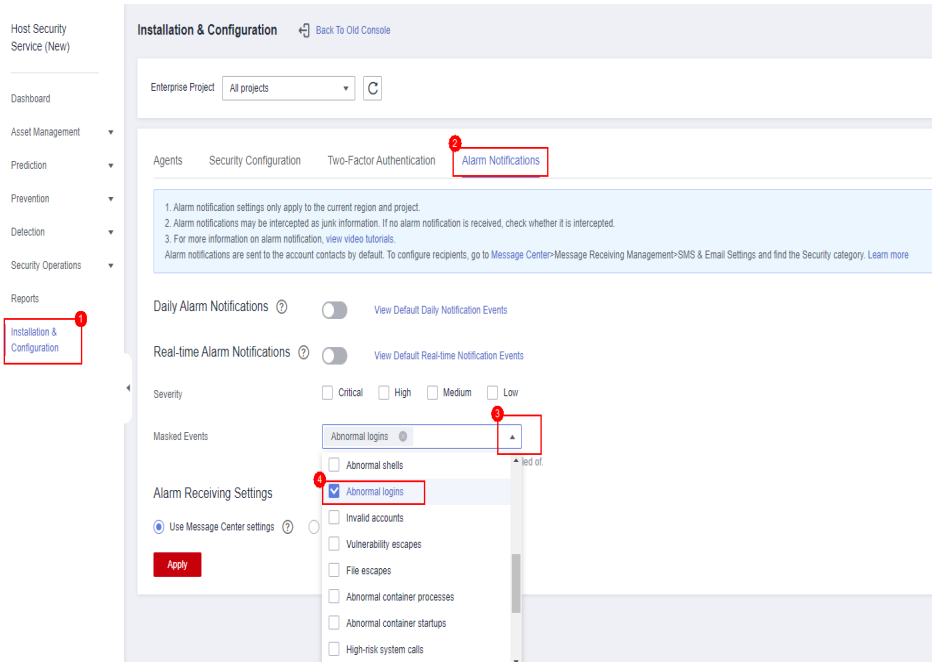
  Figure 5-3 Adding a common login location

- Choose **Installation & Configuration** and click **Alarm Notifications**. In the **Masked Events** box, select **Abnormal logins**.

  Exercise caution when you deselect the **Abnormal Logins** notification item. Abnormal logins include remote logins and successful hacks. If you deselect this item, you will not receive alarms on brute-force attacks in real time.

  Figure 5-4 Deselecting abnormal logins

5.5 How Do I Know Whether an Intrusion Succeeded?

- If you have enabled alarm notifications for intrusion detection, you will be notified immediately when an account is cracked or may be cracked.
- You can also check whether attack IP addresses are blocked on the **Detection & Response** page.
- To further determine the details, perform the following steps:
  - Linux

For Linux servers, you can view logs in **/var/log/secure** and **/var/log/message** directories, or run the **last** command to check whether there are abnormal login records.

- Windows

  To view server login logs, perform the following steps:

  i. Open **Control Panel**.

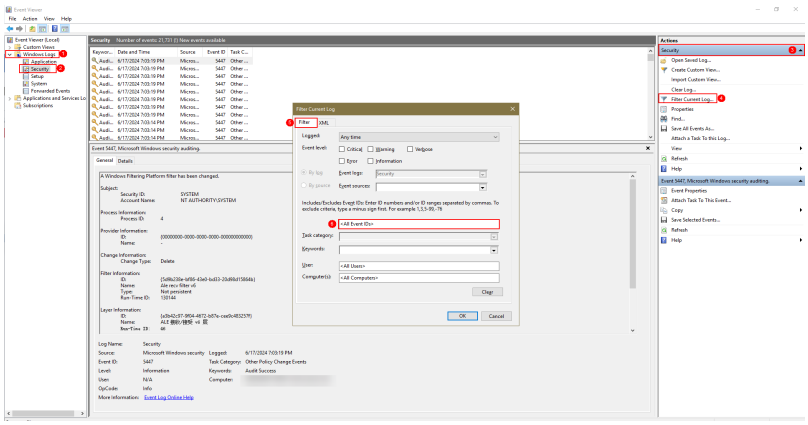
  ii. Choose **Administrative Tools** > **Event Viewer**. The **Event Viewer** page is displayed.

  iii. In the navigation tree on the left, choose **Windows Logs** > **Security**. The **Security** page is displayed.

  iv. In the navigation tree on the right, choose **Security** > **Filter Current Log**. The **Filter Current Log** dialog box is displayed.

  v. On the **Filter** tab, locate the **<All Event IDs>**.

  Figure 5-5 Filter

  vi. Enter the login event ID and click **OK** to filter the target login events.
  - 4624: ID of successful login events
  - 4625: ID of failed login events

6 Brute-force Attack Defense

6.1 How Does HSS Intercept Brute Force Attacks?

Types of Detectable Brute Force Attacks

HSS can detect the following types of brute force attacks:

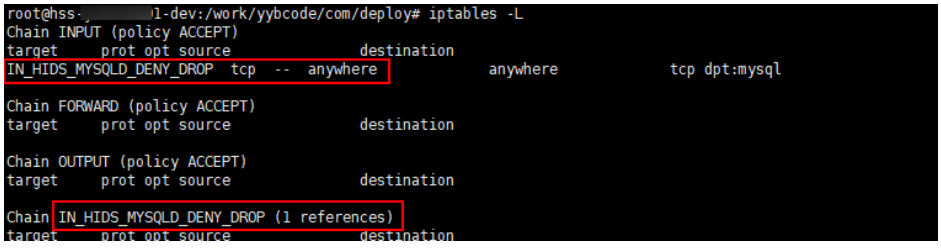
- Windows: SQL Server (automatic interception is not supported currently) and RDP
- Linux: MySQL, vfstpd, and SSH

If MySQL, vfstpd, or SSH is installed on your server, after HSS is enabled, the agent will add rules to iptables to prevent brute force attacks. If a brute-force attack is detected, its source IP address will be added to the blocking list.

- Added MySQL rule: IN_HIDS_MYSQLD_DENY_DROP
- Added vfstpd rule: IN_HIDS_VSFTPD_DENY_DROP
- Added SSH rule: If SSH on the server does not support the TCP Wrapper interception mode, the SSH uses iptables for interception. Therefore, the IN_HIDS_SSHD_DENY_DROP rule will be added to iptables. If you have configured an SSH login whitelist, the IN_HIDS_SSHD_DENY_DROP and IN_HIDS_SSHD_WHITE_LIST will be added to iptables.

Take the MySQL database as an example. **Figure 6-1** shows the new rule.

Figure 6-1 Added MySQL rule



NOTICE

Existing iptables rules are used for blocking brute-force attacks. You are advised to keep them. If they are deleted, HSS will not be able to protect MySQL, vfstpd, or SSH from brute-force attacks.

How Brute Force Attacks Are Intercepted

Brute-force attacks are a type of common intrusion attacks. Attackers submit many server passwords until eventually guessing correctly and gaining control over a server.

HSS uses brute-force detection algorithms and an IP address blacklist to effectively prevent brute-force attacks and block attacking IP addresses. The blocking duration is 12 hours. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked. HSS supports **2FA** to authenticate user identity, effectively preventing attackers from hacking accounts.

You can **set common login IP addresses** and **SSH IP address whitelist** that will not be blocked.

NOTE

If HSS detects account cracking attacks on servers using Kunpeng EulerOS (EulerOS with Arm), it does not block the source IP addresses and only generates alarms. The SSH login IP address whitelist does not take effect for such servers.

Alarm Policies

- If a hacker successfully cracks the password and logs in to a server, a real-time alarm will be immediately sent to specified recipients.
- If a brute-force attack and risks of account hacking are detected, a real-time alarm will be immediately sent to specified recipients.
- If a brute-force attack is detected and failed, and no unsafe settings (such as weak passwords) are detected on the server, no real-time alarms will be sent. HSS will summarize all attacks in a day in its daily alarm report. You can also view blocked attacks on the **Detection & Response** > **Alarms** page of the HSS console.

Viewing Brute Force Cracking Detection Results

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 & Response** > **Alarms**.

Step 4 View the brute force cracking detection result of the server or container.

- View the brute force cracking detection result of the server.
  a. Click the **Server Alarms** tab.

b. In the **Alarm Types** area, select **Abnormal User Behavior** > **Brute-force attacks** to view alarm event records on the protected server.

c. Click the value in the **Blocked IP Addresses** area to view the blocked attack source IP address, attack type, blocking status, blocking times, blocking start time, and latest blocking time.

- **Blocked** indicates the brute-force attack has been blocked by HSS.
- **Canceled** indicates you have unblocked the source IP address of the brute force attack.

NOTE

The default blocking duration is 12 hours. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.

- View the brute force cracking detection result of a container.

a. Click the **Container Alarms** tab.

b. In the **Alarm Types** area, select **Abnormal User Behavior** > **Brute-force attacks** to view alarm event records on the protected container.

----End

Managing Blocked IP Addresses

- If a server is frequently attacked, you are advised to fix its vulnerabilities in a timely manner and eliminate risks.

  You are advised to enable **2FA**, and configure **common login IP addresses** and the **SSH login IP whitelist**.
- If a valid IP address is blocked by mistake (for example, after O&M personnel enter incorrect passwords for multiple times), **manually unblock the IP address**.

NOTICE

If you manually unblocked an IP address, but incorrect password attempts from this IP address exceed the threshold again, this IP address will be blocked again.

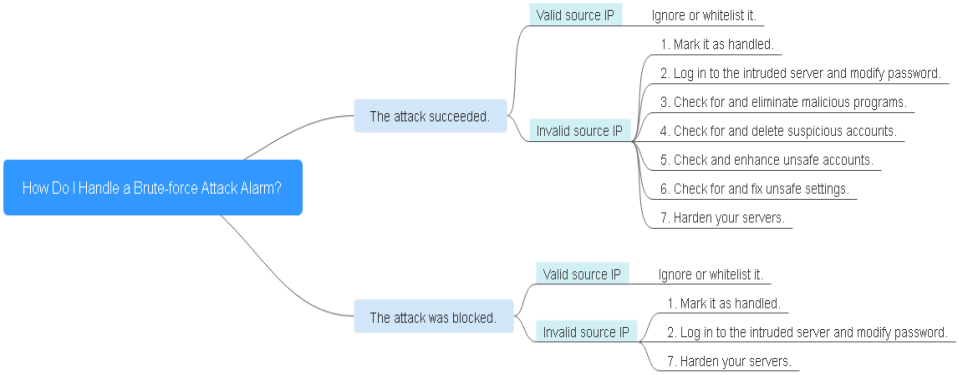
6.2 How Do I Handle a Brute-force Attack Alarm?

- If a brute-force attack succeeded, take immediate measures to prevent attackers from further actions, such as breaching data, performing DDoS attacks, or implanting ransomware, miners, or Trojans.
- If a brute-force attack was blocked, take immediate measures to enhance your servers.

Mind map for troubleshooting

The following mind map describes how to handle a brute-force attack alarm.

Figure 6-2 Mind map for troubleshooting



Handling the Alarm of a Successful Brute-force Attack

If you received an alarm notification indicating that your account had been cracked, you are advised to harden your servers as soon as possible.

Step 1 Log in to the management console.

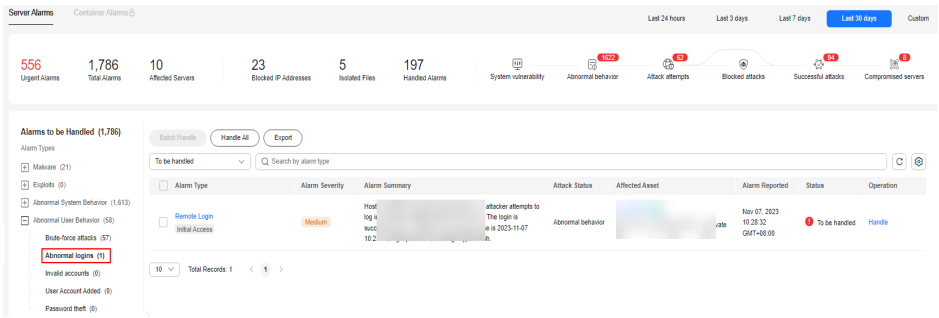
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 Check whether the IP address that triggered the alarm is valid.

1. In the navigation pane, choose **Detection & Response** > **Alarms**.
2. In the **Alarm Types** area, select **Abnormal User Behavior** > **Abnormal logins** to view abnormal login alarm events.
3. Click the alarm event name. On the details page that is displayed, check the login IP address.
   - If the IP address is from a normal user (for example, who entered incorrect password for multiple times but logged in before their account is blocked), your server is not intruded. In this case, you can click **Handle** and ignore the event.
   - If the IP address is invalid, your server may have been intruded.

     In this case, mark this event as handled, log in to the intruded server, and change its password to a stronger one. For details, see **How Do I Set a Secure Password?**

Figure 6-3 Abnormal logins



Step 4 Check for and eliminate malicious programs.

1. In the navigation pane, choose **Detection & Response** > **Alarms**.
2. In the **Alarm Types** area, select **Malware** > **Unclassified malware** to filter the unclassified malware.
3. In the **Alarm Type** column, select **Malicious program** and check alarm events.

   You can click an alarm name to view alarm event details.

   - If you find malicious programs implanted in your servers, locate them based on their process paths, users running them, and startup time.

     To kill a malicious program in an alarm event, click **Handle** in the **Operation** column of an alarm and select **Isolate and kill**.
   - If you have confirmed that all the malicious program alarms are false, go to **Step 5**.

Step 5 Check for suspicious account change records.

1. In the navigation pane on the left, choose **Asset Management** > **Server Fingerprints**.
2. Click the **Account Information** tab. Detect suspicious account change records to prevent attackers from creating accounts or escalating account permissions (for example, adding login permissions to an account)..

Step 6 **Check and handle invalid accounts.**

1. In the navigation pane, choose **Detection & Response** > **Alarms**.
2. In the **Alarm Types** area, select **Abnormal User Behavior** > **Invalid accounts**. View and handle the invalid account alarms. For details, see **Handling Server Alarms**.

Step 7 Check for and fix unsafe settings.

Check for and fix weak password complexity policies and unsafe software settings on your servers. For details, see **Fixing Unsafe Configurations**.

Step 8 Harden your servers.

For more information, see **Hardening Security for SSH Logins to Linux ECSs**.

----End

Handling the Alarm of a Blocked Brute-force Attack

If you have enabled the HSS basic edition or higher, HSS will protect your servers against brute-force attacks.

In the basic edition and higher, you can configure a login security policy to specify the brute force cracking determination mode and blocking duration. For details, see **Login Security Check**.

If you have not configured any login security detection policy, the following default login security policy is used: HSS will block an IP address if it has five or more brute-force attack attempts detected within 30 seconds, or 15 or more brute-force attack attempts detected within 3,600 seconds.

If you receive an alarm indicating that an attack source IP address is blocked, check whether the source IP address is a trusted IP address.

Constraints and Limitations

- Linux

  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
  - 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.

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 **Detection & Response** > **Alarms**. Choose **Abnormal User Behavior** > **Brute-force attacks** to view account brute force events.

Brute-force attack alarms will be generated if:

- The system uses weak passwords, is under brute-force attacks, and attacker IP addresses are blocked.
- Users fail to log in after several incorrect password attempts, and their IP addresses are blocked.

Step 4 Check whether the login IP address triggering the alarm is valid.

- If the source IP address is valid,
  - To handle a false alarm, click **Handle** in the row of the alarm event. Mark this event as **Ignore** or **Add to Login Whitelist**.

    This does not unblock the IP address.
  - To unblock the IP address, click **View Details** under **Blocked IP Addresses**, select the IP address, and unblock it. Alternatively, you can just wait for it to be automatically unblocked when its blocking duration expires. The default blocking duration is 12 hours.
- If the source IP address is invalid or unknown,

  Click **Handle** in the **Operation** column of the brute-force attack event and select **Mark as handled**.

  Immediately log in to your server and change your password to a stronger one. You can also enhance the defense against brute-force attacks by following the instructions provided in **How Do I Defend Against Brute-force Attacks?**

----End

Helpful Links

- How Does HSS Intercept Brute Force Attacks?
- How Do I Unblock an IP Address?

6.3 How Do I Defend Against Brute-force Attacks?

Impact of Account Cracking

Intruders who cracked server accounts can exploit permissions to steal or tamper with data on servers, interrupting enterprise services and causing great loss.

Preventive Measures

- Configure the SSH login whitelist.

  The SSH login whitelist allows logins from only whitelisted IP address, effectively preventing account cracking. For details, see **Configuring an SSH Login IP Address Whitelist**.

- Enable 2FA.

  2FA requires users to provide verification codes before they log in. The codes will be sent to their mobile phones or email boxes.

  Choose **Installation & Configuration**. On the **Two-Factor Authentication** tab, select servers and click **Enable 2FA**. For details, see **Two-Factor Authentication**.

- Use non-default ports.

  Change the default remote management ports 22 and 3389 to other ports.

- Configure security group rules to prevent the attacking IP addresses from accessing your service ports.

  NOTE

  You are advised to allow only specified IP addresses to access open remote management ports (for example, for SSH and remote desktop login).

  You can **configure security group rules** to control access to your servers. For a port used for remote login, you can set IP addresses that are allowed to remotely log in to your ECSs.

  To allow IP address **192.168.20.2** to remotely access Linux ECSs in a security group over the SSH protocol and port 22, you can configure the following security group rule.

  Table 6-1 Setting IP addresses to remotely connect to ECSs

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	For example, 192.168.20.2/32

- Set a strong password.

Password policy check and **weak password detection** can find accounts that use weak passwords on your servers. You can view and handle password risks on the console.

6.4 How Do I Unblock an IP Address?

HSS will block an IP address if it has five or more brute-force attack attempts detected within 30 seconds, or 15 or more brute-force attack attempts detected within 3600 seconds. If a normal IP address is blocked by mistake (for example, after O&M personnel enter incorrect passwords for multiple times), you can unblock the IP address.

If you manually unblocked an IP address, but incorrect password attempts from this IP address reach the threshold again, this IP address will be blocked again.

NOTE

- The default blocking duration is 12 hours.
- If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.

Procedure

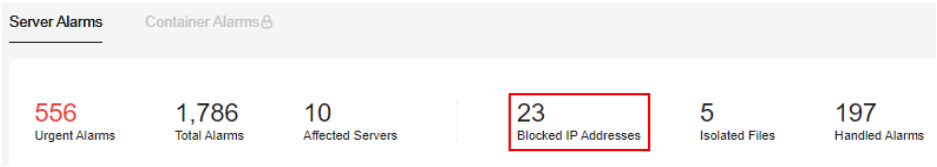
Step 1 Log in to the management console.

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 **Detection & Response** > **Alarms** and click **Server Alarms**.

Step 4 In the **Alarm Statistics** area, click **View Details** under **Blocked IP Addresses**.

Figure 6-4 Blocked IP addresses



Step 5 In the blocked IP address list, select an IP address and click **Cancel Interception**.

----End

6.5 What Do I Do If HSS Frequently Reports Brute-force Alarms?

An alarm indicates that an attack was detected. It does not mean your cloud servers have been intruded. If you receive an alarm, handle it and take countermeasures in a timely manner.

Possible Causes

No access control is configured for the ports used for remotely connecting to your servers. As a result, viruses on the network frequently attacked your ports.

Solution

Take any of the following measures.

- Configure the SSH login whitelist.

  The SSH login whitelist allows logins from only whitelisted IP address, effectively preventing account cracking. For details, see **Configuring an SSH Login IP Address Whitelist**.

- Enable 2FA.

  2FA requires users to provide verification codes before they log in. The codes will be sent to their mobile phones or email boxes.

  Choose **Installation & Configuration**. On the **Two-Factor Authentication** tab, select servers and click **Enable 2FA**. For details, see **Two-Factor Authentication**.

- Use non-default ports.

  Change the default remote management ports 22 and 3389 to other ports.

- Configure security group rules to prevent the attacking IP addresses from accessing your service ports.

  NOTE

  You are advised to allow only specified IP addresses to access open remote management ports (for example, for SSH and remote desktop login).

  You can **configure security group rules** to control access to your servers. For a port used for remote login, you can set IP addresses that are allowed to remotely log in to your ECSs.

  To allow IP address **192.168.20.2** to remotely access Linux ECSs in a security group over the SSH protocol and port 22, you can configure the following security group rule.

  Table 6-2 Setting IP addresses to remotely connect to ECSs

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	For example, 192.168.20.2/32

- Set a strong password.

  Password policy check and **weak password detection** can find accounts that use weak passwords on your servers. You can view and handle password risks on the console.

How Does HSS Intercept Brute Force Attacks?

HSS can detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts.

By default, HSS will block an IP address if it has five or more brute-force attack attempts detected within 30 seconds, or 15 or more brute-force attack attempts detected within 3600 seconds.

If you have enabled an edition higher than HSS basic, you can configure a login security policy to specify the brute force cracking determination mode and blocking duration. For details, see **Login Security Check**.

To view the IP addresses blocked by HSS, choose **Detection & Response** > **Alarms** and click the value above **Blocked IP Addresses**.

6.6 What Do I Do If a Huawei Cloud IP Address Trigger a Brute-force Attack Alarm?

NOTE

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

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

Possible Cause

Some servers users use simple passwords or common ports, or do not use any security protection products. These users' accounts can be easily cracked. Attackers can exploit the accounts and attack other users. In this way, alarms are reported from the IP addresses of the exploited accounts.

Solution

- Restrict access from the IP addresses that triggered alarms. For details, see **Adding a Security Group Rule**.
- When brute-force attacks are detected, they are blocked immediately and alarms are reported. Handle the alarm within seven days, or the EIPs that triggered alarms will be blocked until their alarms are handled.

NOTE

- You can enhance security by setting strong passwords and changing ports. For details, see **How Do I Defend Against Brute-force Attacks?**
- You can purchase HSS to protect your servers. For more information, see **Purchase HSS Quota**. For details about HSS editions, see **Features**.

6.7 What Do I Do If the Port in Brute-force Attack Records Is Not Updated?

Symptom

The remote port of a server has been changed, but the brute-force attack records still displays the old port.

Solution

The remote port configuration is synchronized to HSS through the agent. If the remote port is changed, perform the following operations to restart the agent:

- Windows: Log in to the server as an administrator. Open Task Manager, right-click **HostGuard** and choose **Restart** from the shortcut menu.
- Linux: Run the **/etc/init.d/hostguard restart** command as the **root** user.

7 Baseline Inspection

7.1 Why Are Weak Password Alarms Generated After the Weak Password Detection Policy Is Disabled?

If you have enhanced passwords before disabling the weak password policy, the weak password alarm will not be reported again.

If you do not enhance passwords before disabling the weak password policy, the reported alarm will persist and be retained for 30 days.

- 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.

After modifying weak passwords, you are advised to perform manual detection immediately to verify the result. If you do not perform manual verification and do not disable the weak password scan, HSS will automatically check the settings the next day in the early morning.

7.2 How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS?

Installing a PAM

Your password complexity policy cannot be checked if no pluggable authentication module (PAM) is running on your servers. If PAM is not installed on a server, HSS will prompt you to install it on the **Password Complexity Policy Detection** tab of the **Risk Management** > **Baseline Checks** page.

For Debian or Ubuntu, run the **apt-get install libpam-cracklib** command as the administrator to install a PAM.

NOTE

A PAM is installed and running by default in CentOS, Fedora, and EulerOS.

Setting a Password Complexity Policy

A proper password complexity policy would be: the password must contain at least eight characters and must contain uppercase letters, lowercase letters, numbers, and special characters.

NOTE

The preceding configurations are basic security requirements. For more security configurations, run the following commands to obtain help information in Linux OSs:

- For CentOS, Fedora, and EulerOS based on Red Hat 7.0, run:

  man pam_pwquality

- For other Linux OSs, run:

  man pam_cracklib

- CentOS, Fedora, and EulerOS

  a. Run the following command to edit the **/etc/pam.d/system-auth** file:

  vi /etc/pam.d/system-auth

  b. Find the following information in the file:

  - For CentOS, Fedora, and EulerOS based on Red Hat 7.0:

    password requisite pam_pwquality.so try_first_pass retry=3 type=

  - For other CentOS, Fedora, and EulerOS systems:

    password requisite pam_cracklib.so try_first_pass retry=3 type=

  c. Add the following parameters and their values: **minlen**, **dcredit**, **ucredit**, **lcredit**, and **ocredit**. If the file already has these parameters, change their values. For details, see **Table 7-1**.

  Example:

  password requisite pam_cracklib.so try_first_pass retry=3 minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 type=

  NOTE

  Set **dcredit**, **ucredit**, **lcredit**, and **ocredit** to negative numbers.

Table 7-1 Parameter description

Parameter	Description	Example
minlen	Minimum length of a password. For example, if you want the minimum length to be eight, set the **minlen** value to 8.	minlen=8

Parameter	Description	Example
dcredit	Number of digits A negative value (for example, **-N**) indicates the number (for example, N) of digits required in a password. A positive value indicates that there is no limit.	dcredit=-1
ucredit	Number of uppercase letters A negative value (for example, **-N**) indicates the number (for example, N) of uppercase letters required in a password. A positive value indicates that there is no limit.	ucredit=-1
lcredit	Number of lowercase letters A negative value (for example, **-N**) indicates the number (for example, N) of lowercase letters required in a password. A positive value indicates that there is no limit.	lcredit=-1
ocredit	Number of special characters A negative value (for example, **-N**) indicates the number (for example, N) of special characters required in a password. A positive value indicates that there is no limit.	ocredit=-1

- Debian and Ubuntu
  a. Run the following command to edit the **/etc/pam.d/common-password** file:

     vi /etc/pam.d/common-password

  b. Find the following information in the file:

     password requisite pam_cracklib.so retry=3 minlen=8 difok=3

  c. Add the following parameters and their values: **minlen**, **dcredit**, **ucredit**, **lcredit**, and **ocredit**. If the file already has these parameters, change their values. For details, see **Table 7-1**.

     Example:

     password requisite pam_cracklib.so retry=3 minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 difok=3

7.3 How Do I Set a Proper Password Complexity Policy in a Windows OS?

A proper password complexity policy would be: eight characters for the length of a password and at least three types of the following characters used: uppercase letters, lowercase letters, digits, and special characters.

Perform the following steps to set a local security policy:

Step 1 Log in to the OS as user **Administrator**. Choose **Start** > **Control Panel** > **System and Security** > **Administrative Tools**. In the **Administrative Tools** folder, double-click **Local Security Policy**.

NOTE

- Alternatively, click **Start** and type **secpol.msc** in the **Search programs and files** box.
- When a policy is applied to a server, the domain policy takes precedence over the locally defined policy on the server.

Step 2 Choose **Account Policies** > **Password Policy** and perform the following operations.

- Double-click **Password must meet complexity requirements**, select **Enable**, and click **OK** to enable the policy.
- Double-click **Minimum password length**, enter the length (greater than or equal to **8**), and click **OK** to set the policy.

Step 3 Press **Windows**+**R** to open the **Run** window.

Step 4 Enter **cmd** and click **OK**. The command prompt window is displayed.

Step 5 Run the following command to refresh policies:

gpupdate/force

After the refreshing, the settings will be applied.

----End

7.4 How Do I Handle Unsafe Configurations?

HSS automatically performs a configuration detection for servers. You can repair unsafe configuration items or ignore the configuration items you trust based on the detection result.

- Modifying unsafe configuration items

  View details about a detection rule, verify the detection result based on the audit description, and handle the exception based on the modification recommendation.

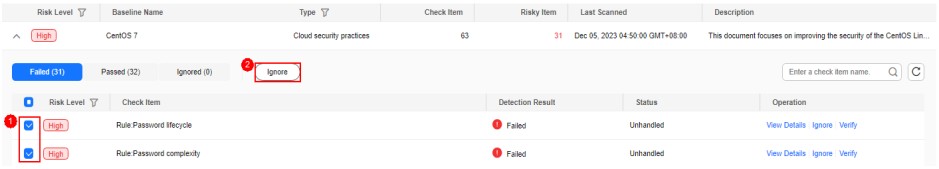
  You are advised to repair the configurations with a high threat level immediately. The configurations with a medium or low threat level can be fixed later based on service requirements.

- Ignoring trusted configuration items
  a. Log in to the management console.
  b. In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.
  c. In the navigation pane, choose **Asset Management** > **Servers & Quota**.

     NOTE

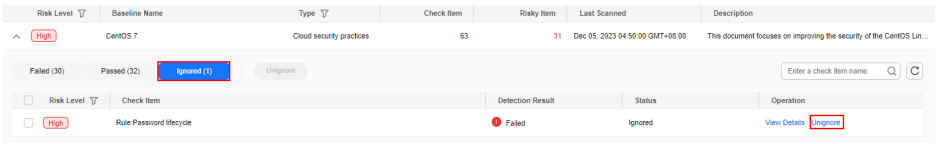
     If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.
  d. On the **Servers** tab, click the name of a server to view its details. Choose **Baseline Checks** > **Unsafe Configurations**.
  e. Locate a baseline item, click ⌄ in front of its name to expand the check items, and click **Ignore** in the **Operation** column of an item. You can also select multiple detection rules and click **Ignore** in the upper part of the page to ignore them in batches.

Figure 7-1 Ignoring a risky configuration



To unignore an ignored detection rule, click **Unignore** in the **Operation** column. You can also select multiple ignored detection rules and click **Unignore** in the upper part of the page to unignore them in batches.

Figure 7-2 Unignoring malicious programs



- Verification

  After a configuration item is fixed, you are advised to click **Verify** in the **Operation** column. After the verification, check the fix result.

7.5 How Do I View Configuration Check Reports?

You can view the configuration check details online.

Viewing the Configuration Check Report

Step 1 Log in to the management console.

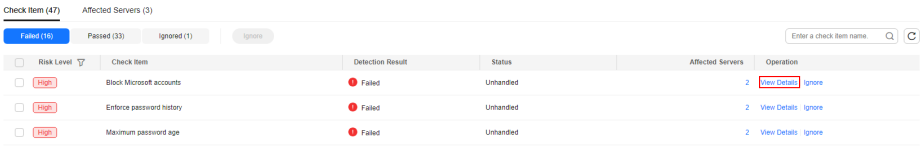
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

Step 3 In the navigation pane on the left, choose **Risk Management** > **Baseline Checks**.

Step 4 On the **Unsafe Configurations** tab, click the baseline name. The details page is displayed.

Step 5 In the row containing the target check item, click **View Details** in the **Operation** column to view the check item details and affected servers.

Figure 7-3 Detection details



Step 6 You can rectify unsafe configuration items and ignore trusted configuration items based on the suggestions provided.

----End

7.6 How Do I Handle a Weak Password Alarm?

Servers using weak passwords are exposed to intrusions. If a weak password alarm is reported, you are advised to change the alarmed password immediately.

Causes

- If simple passwords are used and match those in the weak password library, a weak password alarm will be generated.
- A password used by multiple member accounts will be regarded as a weak password and trigger an alarm.

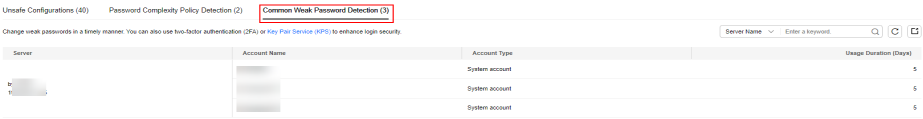
Checking and Changing Weak Passwords

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 **Risk Management** > **Baseline Checks** and click the **Common Weak Password Detection** tab.

Figure 7-4 Common weak passwords



Step 4 Check the server, account name, account type, and usage duration of the weak password. Log in to the server and change the password.

----End

Changing a Weak Password

System	Procedure	Remarks
Windows OS	To change the password in the Windows 10, perform the following steps: 1. Log in to the Windows OS. 2. Click  in the lower left corner and click  . 3. In the **Windows Settings** window, click **Accounts**. 4. Choose **Sign-in options** from the navigation tree. 5. On the **Sign-in options** tab, click **Change** under **Password**.	None
Linux OS	Log in to the Linux server and run the following command: **passwd [<user>]**	If you do not specify any username, you are changing the password of the current user. After the command is executed, enter the new password as prompted. **NOTE** Replace *<user>* with the username.
MySQL database	1. Log in to the MySQL database. 2. Run the following command to check the database user password: **SELECT user, host, authentication_string From user;** This command is probably invalid in certain MySQL versions. In this case, run the following command: **SELECT user, host password From user;** 3. Run the following command to change the password: **SET PASSWORD FOR'*Username*'@'*Host*'=PASSWORD('*New_password*');** 4. Run the following command to refresh password settings: **flush privileges;**	None

System	Procedure	Remarks
Redis database	1. Open the Redis database configuration file **redis.conf**. 2. Run the following command to change the password: **requirepass *<password>*;**	• If there is already a password, the command will change it to the new password. • If there has been no password set, the command will set the password. **NOTE** Replace *<password>* with the new password.
Tomcat	1. Open the **conf/tomcat-user.xml** configuration file in the Tomcat root directory. 2. Change the value of **password** under the **user** node to a strong password.	None

7.7 How Do I Set a Secure Password?

Comply with the following rules:

- Use a password with high complexity.

  The password must meet the following requirements:

  a. Contains at least eight characters.
  b. Contain at least three types of the following characters:
     i. Uppercase letters (A-Z)
     ii. Lowercase letters (a-z)
     iii. Digital (0-9)
     iv. Special characters
  c. The password cannot be the username or the username in reverse order.
- Do not use common weak passwords that are easy to crack, including:
  - Birthday, name, ID card, mobile number, email address, user ID, time, or date
  - Consecutive digits and letters, adjacent keyboard characters, or passwords in rainbow tables
  - Phrases
  - Common words, such as company names, **admin**, and **root**
- Do not use empty or default passwords.
- Do not reuse the latest five passwords you used.
- Use different passwords for different websites and accounts.
- Do not use the same pair of username and password for multiple systems.

- Change your password at least once every 90 days.
- If an account has an initial password, force the user to change the password upon first login or within a limited period of time.
- You are advised to set a locking policy for all accounts. If the consecutive login failures of an account exceed five times, the account will be locked, and will be automatically unlocked in 30 minutes.
- You are advised to set a logout policy. Accounts that have been inactive for more than 10 minutes will be automatically logged out or locked.
- You are advised to force users to change the initial passwords of their accounts upon their first login.
- You are advised to retain account login logs for at least 180 days. The logs cannot contain user passwords.

8 Web Tamper Protection

8.1 Why Do I Need to Add a Protected Directory?

WTP protects files in directories. If no directories are specified, WTP cannot take effect even if it is enabled.

For details, see **Enabling WTP**.

8.2 How Do I Modify 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 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Step 4 Locate the target server and click **Configure Protection** in the **Operation** column.

Step 5 Click **Settings**. On the **Protected Directory Settings** page on the right, select the directory to be edited and click **Edit** in the **Operation** column.

NOTE

- 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 In the **Edit Protected Directory** dialog box, modify the settings and click **OK**.

----End

8.3 What Should I Do If WTP Cannot Be Enabled?

The causes of this problem vary by scenarios.

Agent Status Is Abnormal

- **Symptom**

  The agent status is **Offline** or **Not installed** in the server list on the **Web Tamper Protection** page.

- **Solution**

  Rectify the fault by following the instructions provided in *How Do I Fix an Abnormal Agent*. Ensure that **Agent Status** in the server list is **Online**.

Basic/Enterprise/Premium Edition HSS Has Been Enabled

- **Symptom**

  Protection Status is **Enabled** in the server list on the HSS console.

- **Solution**

  Disable HSS and then enable WTP.

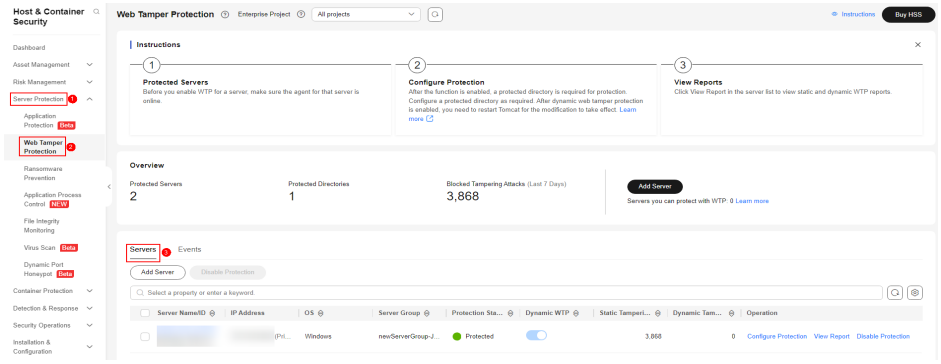
  NOTE

  HSS editions include the basic, enterprise, premium, and WTP editions. Before enabling WTP for a server, ensure that basic, enterprise, or premium edition HSS has been disabled for the server.

Protection Was Enabled on the Wrong Page

To enable WTP, choose **Web Tamper Protection** > **Servers**.

Figure 8-1 Adding protected servers



NOTE

If you have purchasedapplied for the WTP edition, you can use all functions of the premium edition, and you can enable the server protection only on the **Web Tamper Protection**. After WTP is enabled, server protection of the premium edition is also enabled.

8.4 How Do I Modify a File After WTP Is Enabled?

Protected directories are read-only. To modify files or update the website, perform any of the following operations.

Temporarily Disabling WTP

Disable WTP while you modify files in protected directories.

Your website is not protected from tampering while WTP is disabled. Enable it immediately after updating your website.

Setting Scheduled Protection

You can set periodic static WTP, and update websites while WTP is automatically disabled.

Exercise caution when you set the periods to disable WTP, because files will not be protected in those periods.

8.5 What Can I Do If I Enabled Dynamic WTP But Its Status Is Enabled but not in effect?

Dynamic WTP protects your Tomcat applications.

For this function to take effect, ensure that:

- There are Tomcat applications running on your servers.
- Your servers run the Linux OS.
- The **setenv.sh** file has been automatically generated in the **tomcat/bin** directory (usually 20 minutes after you enable dynamic WTP). If the file exists, restart Tomcat to make dynamic WTP take effect.

If the status of dynamic WTP is **Enabled but not in effect** after you enable it, perform the following operations:

- Check whether the **setenv.sh** file has been generated in the **tomcat/bin** directory.
- If the **setenv.sh** file exists, check whether Tomcat has been restarted.

8.6 What Are the Differences Between the Web Tamper Protection Functions of HSS and WAF?

The web tamper protection function of HSS monitors website directories in real time, backs up files, and restores tampered files using the backup, protecting websites from tampering. This function is helpful for governments, educational institutions, and enterprises.

WAF protects user data on the application layer. It supports cache configuration on static web pages. When a user accesses a web page, the system returns a cached page to the user and randomly checks whether the page has been tampered with.

Differences Between the Web Tamper Protection Functions of HSS and WAF

The following table describes the differences between HSS and WAF.

Table 8-1 Differences between the web tamper protection functions of HSS and WAF

Item	HSS	WAF
Static web page protection	• Drive file and web file locking Locks files in driver and web file directories to prevent attackers from tampering with them. • Privileged process management Allows privileged processes to modify web pages.	• Static web pages can be cached on servers. • Privileged process management is not supported.
Dynamic web page protection	Protects your data while Tomcat is running, detecting dynamic data tampering in databases.	No
Backup and restoration	• Active backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local host to restore the file. • Remote backup and restoration If a file directory or backup directory on the local server is invalid, you can use the remote backup service to restore the tampered web page.	No
Suitable for	Websites that have high security requirements and difficult to be manually recovered	Websites that only require application-layer protection

How Do I Select WTP?

Website	Service
Common websites	WAF web tamper protection + HSS enterprise edition
Websites that require strong protection and anti-tampering capabilities	WAF web tamper protection + HSS WTP

9 Container Security

9.1 How Do I Disable Node Protection?

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.

Disabling the Container Edition

Step 1 Log in to the management console.

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

9.2 How Do I Enable Node Protection?

When you enable node protection, the system automatically installs the CGS plug-in on the node.

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 a node, click **Enable Protection**.

Step 5 In the displayed dialog box, read and select **I have read and agree to the Container Guard Service Disclaimer**.

Step 6 Click **OK** to enable protection for the node. If **Protection Status** of the node is **Protected**, protection is enabled for the node.

NOTE

An HSS quota protects one cluster node.

----End

9.3 How Do I Enable the API Server Audit for an On-Premises Kubernetes Container?

Scenario

On-premises Kubernetes containers are used.

Prerequisites

- Container protection has been enabled. For details, see **Enabling Container Node Protection**.
- API server audit is disabled. Perform the following steps to check its status:
  a. Log in to the node where kube-apiserver is located.
  b. Check the **kube-apiserver.yaml** file or the started kube-apiserver process.
     - Go to the **/etc/kubernetes/manifest** directory and check whether **--audit-log-path** and **--audit-policy-file** exist in **kube-apiserver.yaml**. If they do not exist, API server audit is disabled.

- Run the **ps** command to check whether **--audit-log-path** and **--audit-policy-file** exist in the command lines of the kube-apiserver process. If they do not exist, the audit function of the kube-apiserver process is disabled.

Enabling API Server Audit

Step 1 Copy the following YAML content, save it to the YAML file, and name the file **audit-policy.yaml**.

This YAML file is the configuration file of the Kubernetes audit function. You can directly use the file or compile it as needed.

```
apiVersion: audit.k8s.io/v1 # This is required.
kind: Policy
# Don't generate audit events for all requests in RequestReceived stage.
omitStages:
  - "RequestReceived"
rules:
  # The following requests were manually identified as high-volume and low-risk,
  # so drop them.
  # Kube-Proxy running on each node will watch services and endpoint objects in real time
  - level: None
    users: ["system:kube-proxy"]
    verbs: ["watch"]
    resources:
      - group: "" # core
        resources: ["endpoints", "services"]
  # Some health checks
  - level: None
    users: ["kubelet"] # legacy kubelet identity
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes"]
  - level: None
    userGroups: ["system:nodes"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes"]
  - level: None
    users: ["system:apiserver"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["namespaces"]
  # Some system component certificates reuse the master user, which cannot be accurately distinguished from user behavior,
  # considering that subsequent new functions may continue to add system operations under kube-system, the cost of targeted configuration is relatively high,
  # in terms of the overall strategy, it is not recommended (allowed) for users to operate under the kube-system,
  # so overall drop has no direct impact on user experience
  - level: None
    verbs: ["get", "update"]
    namespaces: ["kube-system"]
  # Don't log these read-only URLs.
  - level: None
    nonResourceURLs:
      - /healthz*
      - /version
      - /swagger*
  # Don't log events requests.
  - level: None
    resources:
      - group: "" # core
```



```
      resources: ["events"]
# Don't log leases requests
- level: None
  verbs: [ "get", "update" ]
  resources:
    - group: "coordination.k8s.io"
      resources: ["leases"]
# Secrets, ConfigMaps, and TokenReviews can contain sensitive & binary data,
# so only log at the Metadata level.
- level: Metadata
  resources:
    - group: "" # core
      resources: ["secrets", "configmaps"]
    - group: authentication.k8s.io
      resources: ["tokenreviews"]
# Get responses can be large; skip them.
- level: Request
  verbs: ["get", "list", "watch"]
  resources:
    - group: "" # core
    - group: "admissionregistration.k8s.io"
    - group: "apps"
    - group: "authentication.k8s.io"
    - group: "authorization.k8s.io"
    - group: "autoscaling"
    - group: "batch"
    - group: "certificates.k8s.io"
    - group: "extensions"
    - group: "networking.k8s.io"
    - group: "policy"
    - group: "rbac.authorization.k8s.io"
    - group: "settings.k8s.io"
    - group: "storage.k8s.io"
# Default level for known APIs
- level: RequestResponse
  resources:
    - group: "" # core
    - group: "admissionregistration.k8s.io"
    - group: "apps"
    - group: "authentication.k8s.io"
    - group: "authorization.k8s.io"
    - group: "autoscaling"
    - group: "batch"
    - group: "certificates.k8s.io"
    - group: "extensions"
    - group: "networking.k8s.io"
    - group: "policy"
    - group: "rbac.authorization.k8s.io"
    - group: "settings.k8s.io"
    - group: "storage.k8s.io"
# Default level for all other requests.
- level: Metadata
```

Step 2 Upload the **audit-policy.yaml** file to the **/etc/kubernetes/** directory.

Step 3 Go to the **/etc/kubernetes/manifests** directory and add the following content to the **kube-apiserver.yaml** file to enable API server audit:

```
--audit-policy-file=/etc/kubernetes/audit-policy.yaml
--audit-log-path=/var/log/kubernetes/audit/audit.log
--audit-log-maxsize=100
--audit-log-maxage=1
--audit-log-maxbackup=10
```


NOTE

- **--audit-policy-file**: configuration file used by the audit function.
- **--audit-log-path**: path of the log file where audit events are written. If this flag is not specified, the logging backend will be disabled.
- **--audit-log-maxsize**: maximum size (in MB) of an audit log file before rotation.
- **--audit-log-maxage**: maximum number of days for storing old audit log files.
- **--audit-log-maxbackup**: maximum number of retained audit log files.
- Add the preceding parameters to the **kube-apiserver.yaml** file, ensure that the format of the parameters is the same as that in the **kube-apiserver.yaml** file and cannot contain tab characters.

Step 4 (Optional) If your kube-apiserver runs as a pod, perform the following steps to persist logs on the server:

1. Locate the **volumeMounts** field in **kube-apiserver.yaml** and configure volume mounting as follows:

```
volumeMounts:
  - mountPath: /etc/kubernetes/audit-policy.yaml
    name: audit
    readOnly: true
  - mountPath: /var/log/kubernetes/audit/
    name: audit-log
    readOnly: false
```

2. Locate the **volumes** field in **kube-apiserver.yaml** and configure it as follows:

```
volumes:
- name: audit
  hostPath:
    path: /etc/kubernetes/audit-policy.yaml
    type: File
- name: audit-log
  hostPath:
    path: /var/log/kubernetes/audit/
    type: DirectoryOrCreate
```

----End

9.4 What Do I Do If the Container Cluster Protection Plug-in Fails to Be Uninstalled?

Possible Causes

If the cluster network is abnormal or the plug-in is running, uninstalling the plug-in on the HSS console may fail.

Solution

Perform the following operations on any cluster node to uninstall the container cluster protection plug-in:

Step 1 Log in to a cluster node.

Step 2 Create the file **plugin.yaml** in the **/tmp** directory and copy the following script content to the file:

```
apiVersion: v1
kind: Namespace
```



```
metadata:
  labels:
    admission.gatekeeper.sh/ignore: no-self-managing
    control-plane: controller-manager
    gatekeeper.sh/system: "yes"
    pod-security.kubernetes.io/audit: restricted
    pod-security.kubernetes.io/audit-version: latest
    pod-security.kubernetes.io/enforce: restricted
    pod-security.kubernetes.io/enforce-version: v1.24
    pod-security.kubernetes.io/warn: restricted
    pod-security.kubernetes.io/warn-version: latest
  name: gatekeeper-system
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assign.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assignimage.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assignmetadata.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: configs.config.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constraintpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplatepodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
```



```
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplates.templates.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplate.expansion.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplatepodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: modifyset.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: mutatorpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: providers.externaldata.gatekeeper.sh
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-role
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-role
---
```



```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
  namespace: gatekeeper-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: admissionregistration.k8s.io/v1
kind: MutatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-mutating-webhook-configuration
---
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-validating-webhook-configuration
```

Step 3 Create the file **uninstall.sh** in the **/tmp** directory and copy the following script content to the file:

```
#!/bin/bash
kubectl delete -f /tmp/plugin.yaml
kubectl delete ns cgs-provider
```

Step 4 Run the following command to uninstall the container cluster protection plug-in:

```
bash /tmp/uninstall.sh
```

If information similar to the following is displayed, the plug-in has been uninstalled.


```
namespace "gatekeeper-system" deleted
resourcequota "gatekeeper-critical-pods" deleted
customresourcedefinition.apiextensions.k8s.io "assign.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignimage.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignmetadata.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "configs.config.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constraintpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplates.templates.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplate.expansion.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "modifyset.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "mutatorpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "providers.externaldata.gatekeeper.sh" deleted
serviceaccount "gatekeeper-admin" deleted
role.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
clusterrole.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
rolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
secret "gatekeeper-webhook-server-cert" deleted
service "gatekeeper-webhook-service" deleted
deployment.apps "gatekeeper-audit" deleted
deployment.apps "gatekeeper-controller-manager" deleted
poddisruptionbudget.policy "gatekeeper-controller-manager" deleted
mutatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-mutating-webhook-configuration" deleted
validatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-validating-webhook-configuration" deleted
```

----End

9.5 What Do I Do If the Cluster Connection Component (ANP-Agent) Failed to Be Deployed?

Cluster Connection Component (ANP-Agent) Installation Failure

Symptom

During the access to a third-party cloud cluster or on-premises cluster, the following command is executed to check the installation status of the cluster connection component (ANP-agent):

```
kubectl get pods -n hss | grep proxy-agent
```

The following information is displayed, indicating the cluster connection component (ANP-agent) failed to be installed.

```
proxy-agent-5dc5cf6cd7-khdlt   0/1     ImagePullBackOff     0          42h
proxy-agent-5dc5cf6cd7-n56bx   0/1     Pending              0          42h
```

Solution

Step 1 Log in to a node in the cluster.

Step 2 Run the following command to view the node information:

```
kubectl describe pod proxy-agent-xxx -n hss
```

proxy-agent-*xxx* is the name of the cluster connection component displayed in the command output in "Symptom", for example, **proxy-agent-5dc5cf6cd7-khdlt**.

Step 3 Identify the cause based on the command output.

- **Possible cause**: The image of the cluster connection component cannot be pulled.

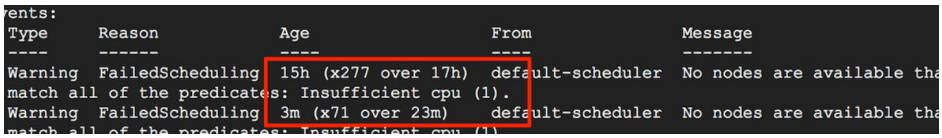
  Figure 9-1 Failed to pull the image of the cluster connection component

  Solution: If you select **Non-CCE cluster (Internet access)**, ensure that your cluster can access the Internet, that is, you can pull the SWR image.

- **Possible cause**: There are not enough CPUs or memory on the node. **Insufficient cpu/memory** is displayed.

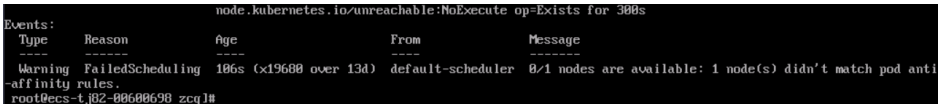
  Figure 9-2 Insufficient CPU or memory

  Solution: Scale up the node and retry access.

- **Possible cause**: There are no nodes matching the scheduling rule.

  Figure 9-3 No nodes matching the scheduling rule

  Solution: For high availability purposes, the cluster connection component (ANP-agent) allocates two instances to different nodes by default. Ensure there are at least two available nodes in the cluster.

----End

Cluster Connection Component (ANP-Agent) Connection Failure

Symptom

During the access to a third-party cloud cluster or on-premises cluster, the following command is executed to check the connection status of the cluster connection component (ANP-agent):

```
for a in $(kubectl get pods -n hss| grep proxy-agent | cut -d ' ' -f1); do kubectl -n hss logs $a | grep 'Start serving';done
```

The command output is empty, indicating the cluster failed to connect to HSS.

Solution

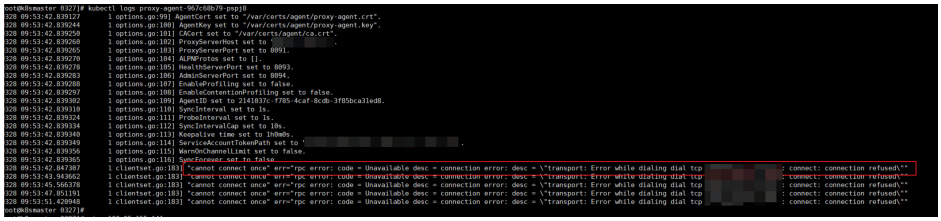
Step 1 Log in to a node in the cluster.

Step 2 Run the following command to check the node logs:

```
kubectl logs proxy-agent-xxx -n hss
```

Step 3 If the command output shown in **Figure 9-4** is displayed, the grpc connection between the cluster connection component and the HSS server failed to be established.

Figure 9-4 Connection failed



Step 4 Perform the following steps to locate and rectify the fault:

NOTE

Format of the server domain name of the cluster connection component: **hss-anp.***region_code***.myhuaweicloud.com**

For details about region codes, see **Regions and Endpoints**.

1. Check whether the cluster security group allows outbound access to port 8091 of the 100.125.0.0/16 CIDR block.
   - If the access is allowed, go to **Step 4.2**.
   - If the access is denied, configure the security group to allow outbound access to the port and retry access.
2. Run the following command to check whether the server domain name of the cluster connection component can be pinged:
   ```
   ping {{Server_domain_name_of_cluster_connection_component}}
   ```
   - If it can be pinged, go to **Step 4.3**.
   - If the IP address cannot be pinged, set the DNS server address to the private DNS server address of Huawei Cloud. For more information, see **Private DNS Server Address of Huawei Cloud**. After the configuration is complete, connect to the cluster asset again.
3. Run the following command to check whether the specified port of the cluster connection component can be accessed:
   ```
   telnet {{Server_domain_name_of_cluster_connection_component}} 8091
   ```
   - If the access is allowed, go to **Step 4.4**.
   - If the access fails, disable the firewall and try again.
4. In the upper right corner of the Huawei Cloud console, choose **Service Tickets** > **Create Service Ticket** and submit a service ticket.

----End

9.6 What Do I Do If Cluster Permissions Are Abnormal?

Symptom

The third-party cloud cluster or on-premises cluster that has been connected to HSS does not have the permission to use the container-related functions provided by HSS.

To check permissions, perform 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 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **Cluster** tab.

Step 5 Click the name of a cluster to go to the cluster node details page and view the permission list.

If **No** is displayed in the **Permissions Assigned** column of a feature, you do not have the permission to use the feature.

----End

Root Causes

A kubeconfig file dedicated to HSS is used by the third-party cloud cluster or on-premises cluster to connect to HSS, but this file is not configured by following the instructions in this document.

Solution

Step 1 Log in to a node in the cluster.

Step 2 Create the **hss-rbac.yaml** file. Copy and save the following content to the file:

```
{"metadata":{"namespace":"hss","name":"hssRole"},"apiVersion":"rbac.authorization.k8s.io/
v1","kind":"Role","rules":[{"resources":["configmaps"],"verbs":
["create","delete","deletecollection","get","list","patch","update","watch"],"apiGroups":[""]},{"resources":
["daemonsets","deployments","deployments/rollback","replicasets"],"verbs":
["create","delete","deletecollection","get","list","patch","update","watch"],"apiGroups":["apps"]},
{"resources":["cronjobs","jobs"],"verbs":
["create","delete","deletecollection","get","list","patch","update","watch"],"apiGroups":["batch"]},
{"resources":["ingresses"],"verbs":
["create","delete","deletecollection","get","list","patch","update","watch"],"apiGroups":["extensions"]},
{"resources":["ingresses"],"verbs":
["create","delete","deletecollection","get","list","patch","update","watch"],"apiGroups":
["networking.k8s.io"]}]}{"metadata":
{"namespace":"hss","name":"hssRoleBinding"},"apiVersion":"rbac.authorization.k8s.io/
v1","kind":"RoleBinding","subjects":[{"kind":"ServiceAccount","name":"hss-
user","namespace":"hss"}],"roleRef":{"apiGroup":"rbac.authorization.k8s.io","kind":"Role","name":"hssRole"}}
{"metadata":{"name":"hssClusterRole"},"apiVersion":"rbac.authorization.k8s.io/
v1","kind":"ClusterRole","rules":[{"resources":
["namespaces","pods","nodes","services","endpoints","configmaps","events","persistentvolumeclaims","persis
tentvolumes","podtemplates","replicationcontrollers","serviceaccounts","pods/log"],"verbs":
["get","list"],"apiGroups":[""]},{"resources":["pods/status"],"verbs":["update"],"apiGroups":[""]},{"resources":
["daemonsets","deployments","replicasets","statefulsets"],"verbs":["get","list"],"apiGroups":["apps"]},
{"resources":["horizontalpodautoscalers"],"verbs":["get","list"],"apiGroups":["autoscaling"]},{"resources":
["cronjobs","jobs"],"verbs":["get","list"],"apiGroups":["batch"]},{"resources":["endpointslices"],"verbs":
["get","list"],"apiGroups":["discovery.k8s.io"]},{"resources":["events"],"verbs":["get","list"],"apiGroups":
["events.k8s.io"]},{"resources":["ingresses"],"verbs":["get","list"],"apiGroups":["extensions"]},{"resources":
["ingressclasses","ingresses","networkpolicies"],"verbs":["create","delete","update","get","list"],"apiGroups":
["networking.k8s.io"]},{"resources":["clusterrolebindings","clusterroles","rolebindings","roles"],"verbs":
["create","delete","deletecollection","patch","update","watch"],"apiGroups":["rbac.authorization.k8s.io"]},
{"resources":["clusterrolebindings","clusterroles","rolebindings","roles"],"verbs":["get","list"],"apiGroups":
["rbac.authorization.k8s.io"]},{"resources":["storageclasses","volumeattachments"],"verbs":
["get","list"],"apiGroups":["storage.k8s.io"]}]}{"metadata":
{"name":"hssClusterRoleBinding"},"apiVersion":"rbac.authorization.k8s.io/
v1","kind":"ClusterRoleBinding","subjects":[{"kind":"ServiceAccount","name":"hss-
user","namespace":"hss"}],"roleRef":
{"apiGroup":"rbac.authorization.k8s.io","kind":"ClusterRole","name":"hssClusterRole"}}
```

Step 3 Run the following command to configure all RBAC permissions required by HSS:

```
kubectl apply -f hss-rbac.yaml
```

Step 4 Log in to the HSS console and check whether the values in the **Permissions Assigned** column are **Yes**. If yes, the permissions are assigned and this fault is rectified.

For details, see the operations for viewing the permission list in **Symptom**.

If you stay on the HSS permission list page during troubleshooting, refresh the page after configuring the permissions.

----End

10 Ransomware Prevention

10.1 What Are the Differences Between Ransomware Protection Backup and Cloud Backup?

The backup of HSS ransomware protection depends on Cloud Backup and Recovery (CBR). The server backup policy takes effect only after CBR is purchased.

There is no difference between the two in terms of backup mechanism and management. The only difference is that ransomware backup generates a dedicated ransomware backup library.

The backup mechanism of ransomware protection inherits that of CBR (Cloud Backup and Restoration). Backup files of ransomware protection can be centrally managed and viewed in CBR.

11 Security Configurations

11.1 How Do I Clear the SSH Login IP Address Whitelist Configured in HSS?

The methods to clear the whitelist vary according to your HSS quota states.

Normal/Expired

Normal and expired quotas can be used. To delete the SSH login IP address, disable or delete it on the management 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 and Compliance** > HSS. The HSS page is displayed.

Step 3 Choose **Installation & Configuration**, click **Security Configuration**, and click **SSH IP Whitelist**.

Step 4 Locate the row that contains the target whitelisted IP address and click **Disable** or **Delete** in the **Operation** column.

----End

Frozen or Deleted After the Freeze Period Expires

If the quota status is **Frozen** or the quota is deleted after the freeze period expired, HSS will no longer protect your servers. You cannot clear the SSH login IP address whitelist through the management console.

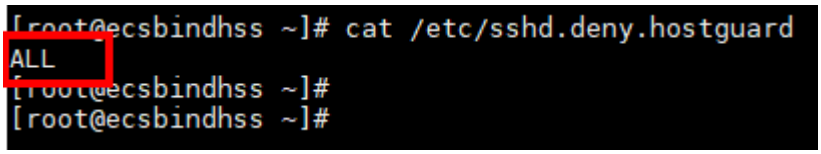
Perform the following steps to clear the configured SSH login IP address whitelist:

Step 1 Log in to the server whose SSH login IP address whitelist needs to be cleared.

Step 2 Run the following command to view the **/etc/sshd.deny.hostguard** file, as shown in **Figure 11-1**.

cat /etc/sshd.deny.hostguard

Figure 11-1 Viewing file content



Step 3 Run the following command to open the **/etc/sshd.deny.hostguard** file:

vim /etc/sshd.deny.hostguard

Step 4 Press **i** to enter the editing mode and delete **ALL**.

Step 5 Press **Esc** to exit the editing mode, and then run the **:wq** command to save the modification and exit.

----End

11.2 What Can I Do If I Cannot Remotely Log In to a Server via SSH?

Symptoms

You can log in to a server via the console but not via SSH.

Possible Causes

- A server will be blocked if it is regarded as a suspicious server performing brute-force attacks (for example, the number of incorrect password attempts reaches 5 within 30 seconds).
- The SSH login IP whitelist is enabled. Your login IP addresses have not been added to the login whitelist.

  If you enable the SSH login IP address whitelist, SSH logins will be allowed only from whitelisted IP addresses.

Solution

Step 1 Check whether your login IP address was blocked because it was regarded as a source of brute-force attacks.

- If yes, perform the following steps:
  a. Log in to the console.
  b. In the navigation pane, choose **Detection & Response** > **Alarms**.
  c. Select the **Server Alarms** tab. Click the value in the **Blocked IP Addresses** area. The **Blocked IP Addresses** page is displayed.
  d. Select the target attack source IP address and click **Unblock** above the list to unblock the IP address.
- If your login IP address was not blocked for this reason, go to **Step 2**.

Step 2 Check whether your login IP address is blocked because it is not whitelisted and the SSH login IP whitelist is enabled.

- If your login IP address was not blocked for this reason, add the IP address to the **SSH login IP address whitelist**.
- If your login IP address was not blocked for this reason, contact technical support.

----End

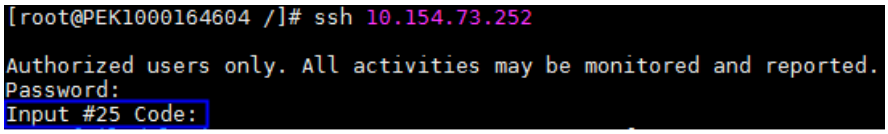
11.3 How Do I Use 2FA?

This FAQ shows you how to use 2FA.

Logging In and Passing 2FA Authentication

- Logging in to a Linux server
  a. Use PuTTY or Xshell to log in to your server.
     Select **Keyboard Interactive** and enter the user identity information.
     - PuTTY
       Set the authentication mode to **Keyboard Interactive** and click **OK**.
     - Xshell
       In the **New Session Properties** dialog box, choose **Connection > Authentication > Method**, choose **Keyboard Interactive** from the **Method** drop-down list, and click **OK**.
  b. Enter the account and password of the server.
  c. Enter the 2FA verification code sent to your terminal.

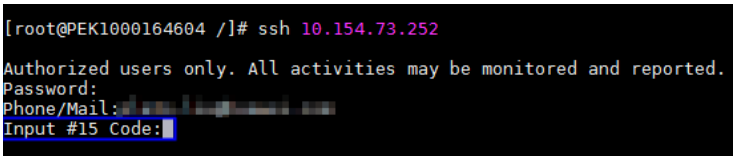
  Figure 11-2 Entering a verification code



NOTE

- The mobile phone or email box subscribed to a notification topic will receive a message: **[Huawei Cloud] Login verification code #** *XX* for your ECS (*xxxx-yyyy*): *XXXXXX*.
- If you do not receive the verification code, check to ensure the SELinux firewall is disabled and try again.
- If HSS detects that a server may be under a brute-force attack, it will ask you to enter detailed information about the subscription terminal (such as the mobile number or email address) before sending a verification code, as shown in **Figure 11-3**.

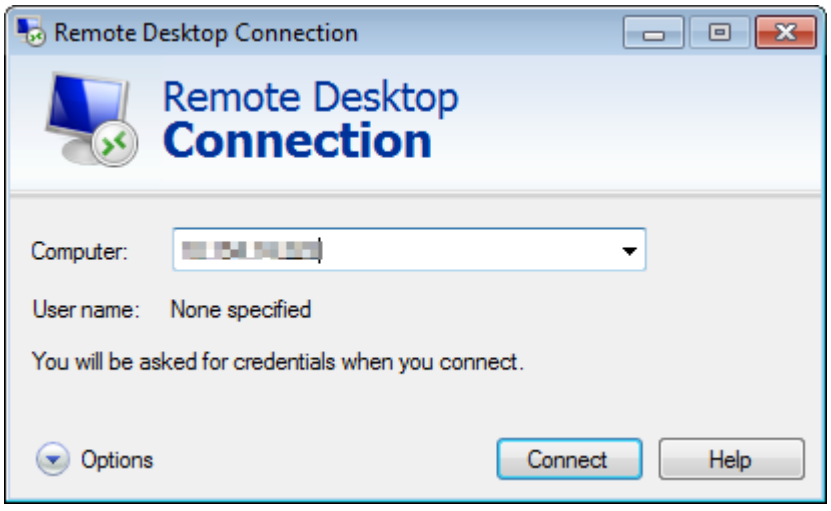
Figure 11-3 Entering a mobile number or email address



- You can add up to 10 mobile numbers and email addresses at a time. A topic can have up to 10,000 mobile numbers and email addresses.

- Logging in to a Windows server
  a. Click **Start**, enter **Remote Desktop Connection** in the search box, and press **Enter** to open the remote desktop connection.
  b. Enter the IP address of the host in the **Computer** text box and click **Connect**.

Figure 11-4 Remote desktop connection



  c. Enter the reserved mobile number or email address to receive 2FA verification code.

NOTE

The mobile phone or email box subscribed to a notification topic will receive a message: **[Huawei Cloud] Login verification code #** *XX* for your ECS (*xxxx-yyyy*): *XXXXXX*.

  d. Enter the verification code, server account name, and password on the login page, and click  to log in to the server.

11.4 What Do I Do If I Cannot Enable 2FA?

Symptoms

- In the 2FA list, there are no servers with disabled 2FA.
- After 2FA is enabled, it does not take effect.
- Failed to enable 2FA.

Possible Causes

- Server protection is not enabled.
- 2FA settings have not taken effect. After 2FA is enabled, it takes about 5 minutes for the settings to take effect.
- For a Linux server, **Key pair** is selected as the login mode.
- 2FA conflicts with G01 or 360 Guard (server edition).
- The SELinux firewall is not disabled.

Solution

Step 1 Check whether HSS has been enabled for the server for which you want to use 2FA.

- If it has, go to **Step 2**.
- If it has not, enable HSS first.

Step 2 Check whether it has been 5 minutes since you enabled 2FA.

- If it has, go to **Step 3**.
- If it has not, wait for 5 minutes and check whether 2FA takes effect.

Step 3 Check whether your server is a Linux server with **Key pair** selected as its login mode.

- If it is, disable the **Key pair** login mode and enable the **Password** login mode.
- If it is not, go to **4**.

Step 4 Check whether the SELinux firewall is disabled on your server.

- If it is, go to **Step 6**.
- If it is not, run either of the following commands to disable it.
  - To temporarily disable the SELinux firewall, run the following command:
    setenforce 0 #Temporarily disable
  - To permanently disable the SELinux firewall, run the following command:
    vi /etc/selinux config
    selinux=disabled #Permanently disable

Step 5 Check whether you have stopped G01 and 360 Guard (server edition) (if any) on your server.

- If you have, go to **Step 6**.
- If you have not, stop the software.

Step 6 Contact technical support.

----End

11.5 Why Can't I Receive a Verification Code After 2FA Is Enabled?

- The two-factor authentication function does not take effect immediately after being enabled.

  Wait for 5 minutes and try again.

- To enable two-factor authentication, you need to disable the SELinux firewall.

  Disable the SELinux firewall and try again.

- Linux servers require user passwords for login.

  To switch from the key login mode to password login mode, perform the following steps:

  a. Use the key to log in to the Linux ECS and set the password of user **root**.

     sudo passwd root

     If the key file is lost or damaged, reset the password of user **root**.

  b. Modify the SSH configuration file on the ECS as user **root**.

     su root

     vi /etc/ssh/sshd_config

     Modify the following settings:

     - Change **PasswordAuthentication no** to **PasswordAuthentication yes**.

       Alternatively, delete the comment tag (#) before **PasswordAuthentication yes**.

     - Change **PermitRootLogin no** to **PermitRootLogin yes**.

       Alternatively, delete the comment tag (#) before **PermitRootLogin yes**.

  c. Restart sshd for the modification to take effect.

     service sshd restart

  d. Restart the ECS. Then, you can log in to the ECS as user **root** using the password.

     NOTE

     To prevent unauthorized users from using the key file to access the Linux ECS, delete the **/root/.ssh/authorized_keys** file or clear the **authorized_keys** file.

11.6 Why Does My Login Fail After I Enable 2FA?

The login failed probably because file configurations or the login mode was incorrect.

Correcting File Configurations

Check whether the configuration file is correct.

Configuration file path: **/etc/ssh/sshd_config**

Configuration items:

PermitEmptyPasswords no

UsePAM yes

ChallengeResponseAuthentication yes

NOTICE

If you use the **root** account for login,the following configuration item is required:

PermitRootLogin yes

Correcting the Login Mode

If you attempted to log in in either of the following ways, your login would fail.

- Used CloudShell to log in to an ECS.
- Attempted to log in to a Linux server through a CBH instance.

Failure cause: 2FA is implemented through a built-in module, which cannot be displayed if you log in in the preceding ways. As a result, the login authentication fails.

Solution: Perform login authentication by referring to **How Do I Use 2FA?**

11.7 How Do I Add a Mobile Number or Email Address for 2FA?

You can set your mobile phone number only if you have selected **SMS/Email** for **Method**. Set your mobile phone number in the SMN topic you choose.

In the **SMN Topic** drop-down list, only the SMN topics with confirmed subscriptions are displayed.

- You can click **View** to go to the SMN console and create a topic. Click **Add Subscription** and enter a mobile phone number or email address.
- You can also add or modify the mobile phone number or email address under an existing topic.
  - Adding a mobile phone number or email address

    Click **View Topics**. Click **Add Subscription** and enter a mobile phone number or email address.
  - Deleting a mobile phone number or email address

    Click **View Topics**. Click a topic name to go to the details page. Click the **Subscriptions** tab and delete one or more target endpoints.

11.8 If I Choose to Use Verification Code for 2FA, How Do I Get the Code?

If you want to enable 2FA is but cannot receive messages through mobile phone or email, you can set **Method** to **Verification code**. Every time you log in to an ECS, HSS will send a random verification code to your login page. You simply need to enter the code to log in.

11.9 Will I Be Billed for Alarm Notifications and SMS?

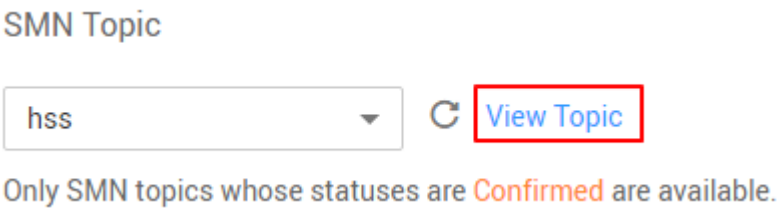
Yes. Simple Message Notification (SMN) is a paid service. For details about the pricing, see **Product Pricing Details**.

11.10 Why No Topics Are Available for Me to Choose When I Configure Alarm Notifications?

No Topics Created

On the **Alarm Notifications** page, click **View Topics** to access the SMN console and create a topic. For details, see **Creating a Topic**.

Figure 11-5 Viewing SMN topics



No Subscribed Topics

After creating a topic, you need to add one or more subscriptions to the topic and confirm the subscriptions as prompted.

11.11 Can I Disable HSS Alarm Notifications?

Yes.

If you do not enable alarm notifications, HSS cannot send alarm notifications to you in a timely manner. To view host security risks, you can only log in to the management console.

Setting Alarm Notifications

After you enable HSS, perform the following operations to configure alarm notifications:

1. Log in to the HSS console.
2. Choose **Installation and Configuration** > **Alarm Notifications**. Configure alarm notifications.

Disabling Alarm Notifications

If you do not want to receive HSS alarm notifications after HSS is enabled, you can disable the notification. After it is disabled, you have to log in to the management console to view alarms.

Use one of the following methods to disable the HSS alarm notification:

- Delete the SMN topic.

  After you delete the topic, your alarm notification settings will not take effect.
- Delete the subscription from the SMN topic.

  After you delete the subscription, you will no longer receive alarm notifications.
- Cancel or disable the subscription from the SMN topic.

  After you cancel the subscription, you will no longer receive alarm notifications.

11.12 How Do I Modify Alarm Notification Items?

If you do not want to receive certain HSS alarm notifications after HSS is enabled, you can disable the notification items. After it is disabled, you have to log in to the management console to view alarms.

Modifying Alarm Notification Items

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 and Configuration**.

Step 4 On the displayed page, click the **Alarm Notifications** tab.

Step 5 Select the events whose alarm notifications are to be masked.

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

To modify multiple notification topics, repeat steps **Step 5** to **Step 6**.

----End

11.13 How Do I Disable the SELinux Firewall?

Security-Enhanced Linux (SELinux) is a kernel module and security subsystem of Linux.

SELinux minimizes the resources that can be accessed by service processes in the system (the principle of least privilege).

Closure Description

- After the SELinux is disabled, services are not affected.
- SELinux can be disabled temporarily or permanently as required.

Scenario

To use the two-factor authentication function of HSS, you need to permanently disable the SELinux firewall.

Procedure

Step 1 Remotely log in to the destination server.

- **Huawei Cloud server**
  - Log in to the ECS console, locate the target server, and click **Remote Login** in the **Operation** column to log in to the server. For details, see **Login Using VNC**.
- **Non-Huawei Cloud server**

  Use a remote management tool (such as PuTTY or Xshell) to connect to the EIP of your server and remotely log in to your server.

Step 2 Run the shutdown command in the command window.

- **Temporarily disable SELinux**

  Run the following command in the CLI to temporarily disable SELinux:

  ```
  setenforce 0
  ```

  NOTE

  After the system is restarted, the SELinux will be enabled again.

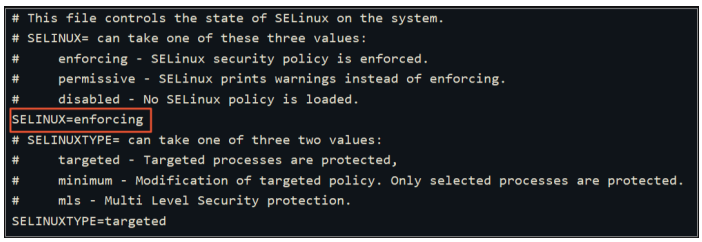
- **Permanently disable SELinux**

  a. Run the following command in the directory window to edit the **config** file of SELinux:

  ```
  vi /etc/selinux/config
  ```

  b. Locate **SELINUX=enforcing**, press **i** to enter the editing mode, and change the parameter to **SELINUX=disabled**.

  Figure 11-6 Editing the SELinux status

  c. After the modification, press **Esc** and run the following command to save the file and exit:

  ```
  :wq
  ```


Step 3 Run the permanent shutdown command, save the settings, and exit. Run the following command to restart the server immediately:

```
shutdown -r now
```

NOTE

The permanent shutdown command takes effect only after the server is restarted.

Step 4 After the restart, run the following command to verify that SELinux is disabled:

```
getenforce
```

----End

12 Protection Quota

12.1 How Do I Extend the Validity Period of HSS Quotas?

The way to increase HSS quota varies by billing mode.

- In pay-per-use mode, you do not need to extend the validity period. You can use as many HSS resources for any duration as needed and will be billed per use.
- In yearly/monthly mode, your quota has a certain validity period. Before the quota expires, you can renew quota.

12.2 How Do I Filter Unprotected Servers?

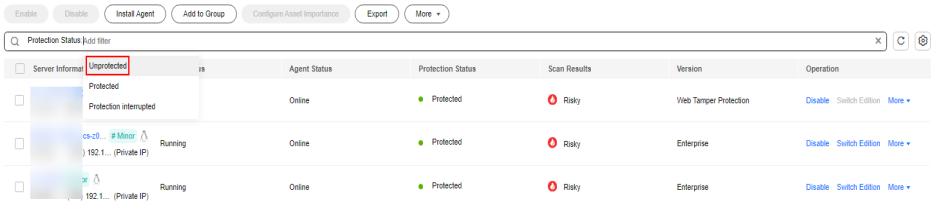
Step 1 Log in to the management console.

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 **Servers**.

Step 4 On the **Servers** tab page, search for servers whose **Protection Status** is **Disabled** and view the unprotected servers.

Figure 12-1 Filtering unprotected servers



----End

12.3 Why Can't I Find the Servers I Purchased on the Console?

You are probably in the wrong region. Only the following servers are displayed on the console:

- Cloud servers purchased in the selected region
- Cloud servers that have been added to the selected region

Solution:

Switch to the correct region before searching for your servers. If enterprise project functions have been enabled for your account, you also need to ensure you have switched to the correct project.

12.4 What Do I Do If My Quotas Are Insufficient and I Failed to Enable Protection?

No Quotas

If you do not have sufficient quotas, quotas in the region where your servers are deployed. For details, see .

Checking Your Page

- To enable the basic, enterprise, or premium edition, choose **HSS** > **Servers**, and enable it on the **Servers** tab.
- If you have purchased the WTP edition, on the HSS console, choose Server Protection > **Web Tamper Protection** and click the **Servers** tab.
- If you have purchased the container edition, on the HSS console, choose **Containers & Quota** and click the **Servers** tab.

Checking Your Project

If enterprise project functions have been enabled for your account, your quota is available only under the project where you purchased it. If you have purchased quotas but cannot find any on the console, switch to the correct project before enabling protection.

12.5 How Do I Allocate My Quota?

The quota can be allocated in the following ways:

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

NOTE

Generally, you can let HSS randomly select a quota.

12.6 If I Change the OS of a Protected Server, Does It Affect My HSS Quota?

No. But before changing the server OS, you need to check whether the HSS agent supports the new OS. To obtain better HSS service experience, you are advised to install or upgrade to an OS version supported by the agent.

HSS agents can run on Linux servers, such as CentOS and EulerOS; and Windows servers, such as Windows 2012 and 2016.

NOTICE

The agent is probably incompatible with the Linux or Windows versions that have reached end of life. To obtain better HSS service experience, you are advised to install or upgrade to an OS version supported by the agent.

Table 12-1 HSS restrictions on Windows (x86)

OS	Agent	System Vulnerability Scan
Windows 10 (64-bit)	√ **NOTE** Only Huawei Cloud Workspace can use this OS.	×
Windows 11 (64-bit)	√ **NOTE** Only Huawei Cloud Workspace can use this OS.	×
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)	√	√
Windows Server 2016 Standard 64-bit English (40 GB)	√	√

OS	Agent	System Vulnerability Scan
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 2019 Datacenter 64-bit English (40 GB)	√	√
Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	√	√
Windows Server 2022 Datacenter 64-bit English (40 GB)	√	×
Windows Server 2022 Datacenter 64-bit Chinese (40 GB)	√	×

Table 12-2 HSS restrictions on Linux (x86)

OS	Agent	System Vulnerability Scan
CentOS 7.4 (64-bit)	√	√
CentOS 7.5 (64-bit)	√	√
CentOS 7.6 (64-bit)	√	√
CentOS 7.7 (64-bit)	√	√
CentOS 7.8 (64-bit)	√	√
CentOS 7.9 (64-bit)	√	√
CentOS 8.1 (64-bit)	√	×
CentOS 8.2 (64-bit)	√	×
CentOS 8 (64-bit)	√	×
CentOS 9 (64-bit)	√	×
Debian 9 (64-bit)	√	√
Debian 10 (64-bit)	√	√
Debian 11.0.0 (64-bit)	√	√
Debian 11.1.0 (64-bit)	√	√

OS	Agent	System Vulnerability Scan
Debian 12.0.0 (64-bit)	√	×
EulerOS 2.2 (64-bit)	√	√
EulerOS 2.3 (64-bit)	√	√
EulerOS 2.5 (64-bit)	√	√
EulerOS 2.7 (64-bit)	√	×
EulerOS 2.9 (64-bit)	√	√
Fedora 28 (64-bit)	√	×
Fedora 31 (64-bit)	√	×
Fedora 32 (64-bit)	√	×
Fedora 33 (64-bit)	√	×
Fedora 34 (64-bit)	√	×
Ubuntu 16.04 (64-bit)	√	√
Ubuntu 18.04 (64-bit)	√	√
Ubuntu 20.04 (64-bit)	√	√
Ubuntu 22.04 (64-bit)	√	√
Ubuntu 24.04 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
Red Hat 7.4 (64-bit)	√	×
Red Hat 7.6 (64-bit)	√	×
Red Hat 8.0 (64-bit)	√	×
Red Hat 8.7 (64-bit)	√	×
OpenEuler 20.03 LTS (64-bit)	√	×
OpenEuler 22.03 SP3 (64-bit)	√	×
OpenEuler 22.03 (64-bit)	√	×

OS	Agent	System Vulnerability Scan
AlmaLinux 8.4 (64-bit)	√	√
AlmaLinux 9.0 (64-bit)	√	×
Rocky Linux 8.4 (64-bit)	√	×
Rocky Linux 8.5 (64-bit)	√	×
Rocky Linux 9.0 (64-bit)	√	×
HCE 1.1 (64-bit)	√	√
HCE 2.0 (64-bit)	√	√
SUSE 12 SP5 (64-bit)	√	√
SUSE 15 (64-bit)	√	×
SUSE 15 SP1 (64-bit)	√	√
SUSE 15 SP2 (64-bit)	√	√
SUSE 15 SP3 (64-bit)	√	×
SUSE 15.5 (64-bit)	√	×
SUSE 15 SP6 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
Kylin V10 (64-bit)	√	√
Kylin V10 SP3 (64-bit)	√	×
UnionTech OS 1050u2e	√ **NOTE** Currently, file escape detection is not supported.	√

Table 12-3 HSS restrictions on Linux (Arm)

OS	Agent	System Vulnerability Scan
CentOS 7.4 (64-bit)	√	√
CentOS 7.5 (64-bit)	√	√

OS	Agent	System Vulnerability Scan
CentOS 7.6 (64-bit)	√	√
CentOS 7.7 (64-bit)	√	√
CentOS 7.8 (64-bit)	√	√
CentOS 7.9 (64-bit)	√	√
CentOS 8.0 (64-bit)	√	×
CentOS 8.1 (64-bit)	√	×
CentOS 8.2 (64-bit)	√	×
CentOS 9 (64-bit)	√	×
EulerOS 2.8 (64-bit)	√	√
EulerOS 2.9 (64-bit)	√	√
Fedora 29 (64-bit)	√	×
Ubuntu 18.04 (64-bit)	√	×
Ubuntu 24.04 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
Kylin V7 (64-bit)	√	×
Kylin V10 (64-bit)	√	√
HCE 2.0 (64-bit)	√	√
UnionTech OS V20 (64-bit)	√	√ **NOTE** Only UnionTech OS V20 server editions E and D support system vulnerability scan.

12.7 Why Doesn't an HSS Edition Take Effect After Purchase?

After purchasing HSS, you need to perform the following operations to make HSS take effect:

1. Install an agent on the target server. After the installation, HSS can monitor the server and report alarms. If you have installed the agent, skip this step.
2. Bind quota: Bind the purchased edition quota to a server to protect it..

After protection is enabled, you are advised to enable alarm notification, so that you can receive notifications once alarms are reported. You are also advised to configure the security parameters for your servers.

12.8 How Do I Change the Protection Quota Edition Bound to a Server?

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.

Switching the HSS Quota Edition

Step 1 Log in to the management console.

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **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 12-4**.

Table 12-4 Parameters for switching editions

Parameter	Description
Billing Mode	Billing mode of a quota. ■ Yearly/Monthly ■ Pay-per-use
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 details about the differences between the editions, see **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.

Parameter	Description
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).

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 12-4**.
  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.

13 Others

13.1 How Do I Use the Windows Remote Desktop Connection Tool to Connect to a Windows Server?

To use the Windows remote connection tool to connect to a Windows server, perform the following steps:

Step 1 On the local PC, choose **Startup** > **Running**, and then run the **mstsc** command to start Windows Remote Desktop Connection.

Step 2 Click **Options**, and then click the **Local Resources** tab. In the **Local devices and resources** area, select **Clipboard**.

Step 3 Click the **General** tab. In **Computer**, enter the EIP of the server on which you want to install an agent. In **User name**, enter **Administrator**. Then click **Connect**.

Step 4 In the displayed dialog box, enter the user password of the server and click **OK** to connect to the server.

----End

13.2 How Do I Check HSS Log Files?

Log Path

The following table describes log files and their paths.

OS	Log Directory	Log File
Linux	/var/log/hostguard/	• hostwatch.log • hostguard.log • upgrade.log • hostguard-service.log • config_tool.log • engine.log
Windows	C:\Program Files\HostGuard\log	• hostwatch.log • hostguard.log • upgrade.log

Log Retention

Log File	Description	Maximum Size	Retained File	Retention Period
hostwatch.log	Records logs generated during the running of daemon processes.	10MB	Latest eight files	Until the HSS agent is uninstalled
hostguard.log	Records logs generated during the running of working processes.	10MB	Latest eight files	
upgrade.log	Records logs generated during version upgrading.	10MB	Latest eight files	
hostguard-service.log	Records logs (scripts) generated when the service starts.	100kB	Latest two logs	
config_tool.log	Records logs (programs) generated when the service starts.	10kB	Latest two logs	
engine.log	Records logs generated when the service exits.	10kB	Latest two logs	

13.3 How Do I Enable Logging for Login Failures?

MySQL

The account hacking prevention function for Linux supports MySQL 5.6 and 5.7. Perform the following steps to enable logging for login failure:

Step 1 Log in to the host as the **root** user.

Step 2 Run the following command to query the **log_warnings** value:

show global variables like 'log_warnings'

Step 3 Run the following command to change the **log_warnings** value:

set global log_warnings=2

Step 4 Modify the configuration file.

- For a Linux OS, modify the **my.conf** file by adding **log_warnings=2** to **[MySQLd]**.

----End

vsftp

This section shows you how to enable logging for vsftp login failures.

Step 1 Modify the configuration file (for example, **/etc/vsftpd.conf**) and set the following parameters:

vsftpd_log_file=log/file/path

dual_log_enable=YES

Step 2 Restart the vsftp service. If the setting is successful, log records shown in the logs shown in **Figure 13-1** will be returned when you log in to vsftp.

Figure 13-1 Log Records

```
Wed Aug 29 14:53:05 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"
Wed Aug 29 14:53:11 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"
Wed Aug 29 14:55:14 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"
Wed Aug 29 14:55:18 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"
Wed Aug 29 14:55:26 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"
Wed Sep  5 11:50:16 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"
Wed Sep  5 11:50:23 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"
Wed Sep  5 13:59:53 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"
Wed Sep  5 13:59:59 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"
Wed Sep  5 14:00:08 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"
```

----End

13.4 How Do I Clear an Alarm on Critical File Changes?

If you are sure the changes on your critical files are safe, you do not need to handle the alarm. It will be automatically cleared in seven days.

13.5 Is HSS Available as Offline Software?

No.

13.6 Why Can't I View All Projects in the Enterprise Project Drop-down List?

Only the accounts with the **Tenant Administrator** permission or **HSS Administrator**+**Tenant Guest** permissions can select **All projects**. If your account does not have the required permissions, you cannot view all enterprise projects. For details about how to grant permissions, see **Assigning Permissions to an IAM User**.

13.7 How Do I Enable or Disable HSS Self-Protection?

HSS self-protection provides the following functions:

- Self-protection in Windows: Prevent malicious programs from uninstalling the agent, tampering with HSS files, or stopping HSS processes.
- Self-protection in Linux: Prevent malicious programs from stopping HSS processes or uninstalling HSS agents.

Self-protection is disabled by default. To enable or disable this function, perform the operations described in this section.

Constraints

- HSS self-protection is available only in the HSS premium or web tamper protection edition, and can be used only if the Linux agent version is 3.2.12 or later or the Windows agent version is 4.0.18 or later.
- Self-protection in Windows depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled. For more details, see:
  - **Enabling Ransomware Prevention**.
  - Antivirus detection and HIPS detection are enabled by default. If you manually disable the two detection items, enable them again by referring to **Viewing a Policy Group**.
- Enabling the self-protection policy has the following impacts:
  - The agent cannot be uninstalled on the control panel of a Windows server. It can be uninstalled on the HSS console.
  - In the agent installation path **C:\Program Files\HostGuard** on a Windows server, you can only access the **log** and **data** directories (and the **upgrade** directory, if your agent has been upgraded).
  - On a Linux server, the agent cannot be uninstalled using commands. It can be uninstalled on the HSS console.

- If you run a command on a Linux server to stop or restart HSS, you need to enter a verification code, which is displayed in the command output after you run the stop or restart command.
- Hide the process information of HSS.

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**.

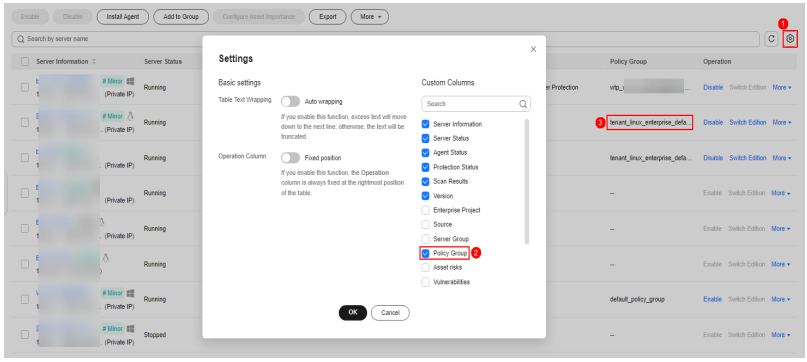
Step 3 In the navigation tree on the left, choose **Security Operations** > **Policies**

Step 4 Click the name of a premium edition policy group for Windows servers. The policy group details page is displayed.

Select the policy group of the server where you want to enable self-protection.

- If you have not created any policy groups of premium edition, you can select the default policy group of the premium or WTP edition. The group name format is **tenant**_*XXX*_*XXX*_**default_policy_group**.
- If you have created policy groups of premium edition, select the policy group of your server. Perform the following operations:
  a. In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**.
  b. Click the **Servers** tab to view the policy groups of servers.

Figure 13-2 Viewing the policy groups of servers



Step 5 In the row containing the target self-protection policy, click **Enable** or **Disable** in the **Operation** column.

Step 6 In the displayed dialog box, click **OK**.

----End

Related Operations

Disabling HSS Self-Protection

Step 1 In the row containing the target self-protection policy, click **Disable** in the **Operation** column.

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

----End

13.8 What Do I Do If Windows Self-Protection Cannot Be Disabled?

Root Causes

If the server network is disconnected, agents cannot receive the command for disabling self-protection delivered by the HSS console. Therefore, HSS self-protection cannot be disabled.

Solutions

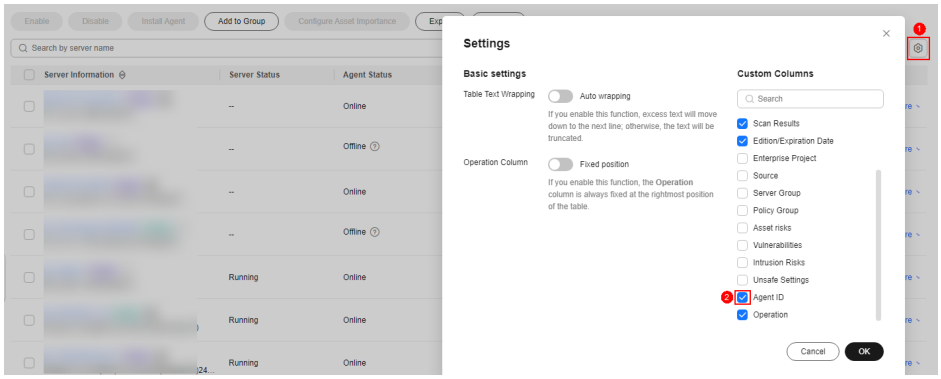
Step 1 Log in to the management console.

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**.

Step 4 Click the **Servers** tab, click in the upper right corner of the server list and select **Agent ID**.

Figure 13-3 Displaying the agent ID



Step 5 Above the server list, enter a server name or ID and click to search for the Windows server for which you want to disable the HSS self-protection.

Step 6 In the row of the target Windows server, copy the first eight characters from the **Agent ID** column.

Step 7 Run **cmd** as the administrator.

Step 8 Run the following command to disable HSS self-protection:

"C:\Program Files\HostGuard\bin\HssClient.exe"1234abcd

NOTE

1234abcd in the command indicates the first eight characters of the agent ID. The first eight characters of the agent ID are used as the verification code when **HSSClient.exe** is executed. It is to prevent malicious programs from disabling self-protection and user misoperations. Self-protection can be disabled only when the first eight characters of the agent ID are correct.

Step 9 If **Disable self protect succeed.** is displayed, HSS self-protection is disabled successfully.

----End

13.9 Why Is a Deleted ECS Still Displayed in the HSS Server List?

After an ECS is deleted, HSS does not synchronize its information immediately. Therefore, you may still see the deleted ECS in the HSS server list. The server list update mechanism is as follows:

- A synchronization task is automatically performed in the early morning every day to refresh the server list.
- HSS starts synchronization immediately when you go to the **Asset Management** > **Servers & Quota** page and will complete synchronization in about 10 minutes. You can then refresh the **Servers & Quota** page and view the latest server list.

