# Host Security Service

# FAQs

**Issue** 38

**Date** 2022-02-11



**HUAWEI TECHNOLOGIES CO., LTD.**

**Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.**

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

## Trademarks and Permissions


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

## Notice

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

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

# Contents

**1 About HSS ..... 1**
1.1 What Is Host Security Service? ..... 1
1.2 Where Is HSS Available? ..... 2
1.3 How Do I Use HSS? ..... 3
1.4 Can I Upgrade My HSS Edition? ..... 3
1.5 Can HSS Protect Local IDC Servers? ..... 4
1.6 Does the HSS Agent Conflict with Any Other Security Software? ..... 4
1.7 What Are the Differences Between HSS, VSS, and WAF? ..... 4
1.8 Can HSS Quota Be Shared Between Accounts? ..... 5
1.9 What Is the HSS Agent? ..... 7
1.10 Can HSS Quota Be Shared Across Regions? ..... 8
1.11 Can I Use HSS If My Services Are Not Deployed on HUAWEI CLOUD? ..... 8
1.12 Can HSS Protect Offline Servers Using the Same Public IP Address? ..... 13
1.13 What HSS Edition Should I Choose to Earn DJCP L2 Certification? ..... 13
1.14 Do I Need to Install Antivirus Software If I Have Enabled HSS? ..... 13
1.15 What Are the Differences Between HSS and SA Baseline Checks? ..... 14
1.16 Can I Add an IP Blacklist in HSS? ..... 15
1.17 Do I Need to Enable HSS Again After My Server OS Is Reinstalled? ..... 15
1.18 How Often Does HSS Detect, Isolate, and Kill Malicious Programs? ..... 16
1.19 How Often Are the HSS Virus Database and Vulnerability Database Updated? ..... 16
1.20 Do I Have to Deploy HSS on All My Cloud Servers? ..... 16
1.21 How Do I Enable the HSS Basic Edition Free of Charge? ..... 17
1.22 How Does HSS Transfer Data? ..... 18
**2 HSS Purchase ..... 19**
2.1 How Can I Use the Free HSS Included with ECS? ..... 19
2.2 Why Can't I Select Free HSS When Purchasing ECS? ..... 20
2.3 How Do I Purchase and Enable HSS? ..... 22
**3 Deployment and Configuration ..... 23**
3.1 Agent ..... 23
3.1.1 Do I Need to Install the HSS Agent After Purchasing HSS? ..... 23
3.1.2 How Do I Install the Agent? ..... 23
3.1.3 How Do I Install the Agent on Servers in Batches? ..... 24

 Copyright © Huawei Technologies Co., Ltd. 

3.1.4 How Do I Install the Agent from the Command Line (on Windows)?....27
3.1.5 Is the Agent in Conflict with Any Other Security Software?....28
3.1.6 What Is the Default Agent Installation Path?....28
3.1.7 How Do I Filter Servers Where No Agents Have Been Installed?....28
3.1.8 What Do I Do If Agent Installation Fails?....29
3.1.9 How Do I Fix an Abnormal Agent?....32
3.1.10 How Many CPU and Memory Resources Are Occupied by the Agent When It Performs Scans?....34
3.1.11 Does HSS Agent Installation Affect My Services?....34
3.1.12 Do WTP and HSS Use the Same Agent?....34
3.1.13 How Do I Uninstall the Agent?....34
3.2 Security Configurations....37
3.2.1 How Do I Clear the SSH Login IP Address Whitelist Configured in HSS?....37
3.2.2 What Can I Do If I Cannot Remotely Log In to a Server via SSH?....39
3.3 Two-factor Authentication (2FA)....39
3.3.1 How Do I Use 2FA?....39
3.3.2 What Do I Do If I Cannot Enable 2FA?....43
3.3.3 Why Can't I Receive a Verification Code After 2FA Is Enabled?....44
3.3.4 Why Does My Login Fail After I Enable 2FA?....44
3.3.5 How Do I Configure My Mobile Number When Enabling 2FA?....45
3.3.6 If I Choose to Use Verification Code for 2FA, How Do I Get the Code?....45
3.4 HSS Quota....46
3.4.1 How Do I Check My Quotas?....46
3.4.2 How Do I Know Whether HSS Has Been Enabled for My Servers?....50
3.4.3 How Do I Filter Unprotected Servers?....50
3.4.4 Why Can't I Find the Servers I Purchased on the Console?....51
3.4.5 What Do I Do If My Quotas Are Insufficient and I Failed to Enable Protection?....51
3.4.6 How Do I Allocate a My Quota?....52
3.4.7 If I Change the OS of a Protected Server, Does It Affect My HSS Quota?....52
3.5 Alarm Notifications....54
3.5.1 Will I Be Billed for Alarm Notifications and SMS?....54
3.5.2 How Do I Modify Alarm Notification Recipients?....54
3.5.3 Why No Topics Are Available for Me to Choose When I Configure Alarm Notifications?....56
3.5.4 Can I Disable HSS Alarm Notifications?....56
3.5.5 How Do I Modify Alarm Notification Items?....57

**4 Alarm and Event Management....61**

4.1 How Do I View and Handle Alarms Reported by HSS?....61
4.2 Brute-force Attack Defense....61
4.2.1 How Does HSS Block Brute-Force Attacks?....61
4.2.2 How Do I Handle a Brute-force Attack Alarm?....64
4.2.3 How Do I Defend Against Brute-force Attacks?....68
4.2.4 What Do I Do If the Account Cracking Prevention Function Does Not Take Effect on Some Accounts for Linux Servers?....70

 Copyright © Huawei Technologies Co., Ltd. 

4.2.5 How Do I Unblock an IP Address?.....71
4.2.6 What Do I Do If HSS Frequently Reports Brute-force Alarms?.....72
4.2.7 How Do I Handle Alarms on the Brute-Force Attacks Launched from a HUAWEI CLOUD IP Address?.....72
4.3 Weak Passwords and Unsafe Accounts.....73
4.3.1 How Do I Handle a Weak Password Alarm?.....73
4.3.2 How Do I Set a Secure Password?.....75
4.3.3 Why Are the Weak Password Alarms Still Reported After the Weak Password Policy Is Disabled?.....76
4.4 Intrusions.....77
4.4.1 What Do I Do If My Servers Are Subjected to a Mining Attack?.....77
4.4.2 Why a Process Is Still Isolated After It Was Whitelisted?.....83
4.4.3 What Should I Do If a Mining Process Is Detected on a Server?.....84
4.4.4 What Should I Do If I Find My Servers Attacking Others?.....84
4.4.5 Why Some Attacks on Servers Are Not Detected?.....84
4.4.6 Can I Unblock an IP Address Blocked by HSS, and How?.....84
4.4.7 Why a Blocked IP Address Is Automatically Unblocked?.....85
4.5 Abnormal Logins.....85
4.5.1 Why Do I Still Receive Remote Login Alarms After Configuring the Login IP Whitelist?.....85
4.5.2 How Do I Check the User IP address of a Remote Login?.....86
4.5.3 What Can I Do If an Alarm Indicating Successful Login Is Reported?.....87
4.5.4 Can I Disable Remote Login Detection?.....87
4.5.5 How Do I Know Whether an Intrusion Succeeded?.....88
4.6 Unsafe Settings.....89
4.6.1 How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS?.....89
4.6.2 How Do I Set a Proper Password Complexity Policy in a Windows OS?.....91
4.6.3 How Do I Handle Unsafe Configurations?.....94
4.6.4 How Do I View Configuration Check Reports?.....94
4.6.5 Do I Need to Handle Detected Configuration Problems of the Windows OS?.....96

**5 Vulnerability Management.....97**

5.1 How Do I Fix Vulnerabilities?.....97
5.2 What Do I Do If an Alarm Still Exists After I Fixed a Vulnerability?.....97
5.3 Why a Server Displayed in Vulnerability Information Does Not Exist?.....99
5.4 Do I Need to Restart a Server After Fixing its Vulnerabilities?.....99
5.5 How Do I Check Vulnerability Severity?.....99
5.6 Can I Check the Vulnerability and Baseline Fix History on HSS?.....100

**6 Web Tamper Protection.....101**

6.1 Why Do I Need to Add a Protected Directory?.....101
6.2 How Do I Modify a Protected Directory?.....101
6.3 What Should I Do If WTP Cannot Be Enabled?.....103
6.4 How Do I Modify a File After WTP Is Enabled?.....104
6.5 What Can I Do If I Enabled Dynamic WTP But Its Status Is Enabled but not in effect?.....105
6.6 What Are the Differences Between the Web Tamper Protection Functions of HSS and WAF?.....105

 Copyright © Huawei Technologies Co., Ltd. 

**7 Enterprise Project ..... 107**
7.1 How Do I Migrate Settings Between Projects After Enabling Enterprise Projects for HSS? ..... 107
7.2 Can I Bind a Server to an HSS Quota If They Are in Different Enterprise Projects? ..... 117

**8 Fee ..... 123**
8.1 Pricing Standards ..... 123
8.2 If I Do Not Renew HSS After It Expires, Will My Services Be Affected? ..... 123
8.3 If I Unsubscribe from HSS and Purchase It Again, Do I Need to Install Agents and Configure Server Protection Settings from Scratch? ..... 123
8.4 How Do I Renew HSS? ..... 124
8.5 How Do I Apply for Unsubscription and Refund? ..... 125

**9 Others ..... 126**
9.1 What Are Regions and AZs? ..... 126
9.2 What Should I Do If the Key Board Response Is Slow or If I Need to Enter Consecutive Digits in Chinese Windows OS? ..... 127
9.3 How Do I Use the Windows Remote Desktop Connection Tool to Connect to a Server? ..... 128
9.4 How Do I Check HSS Log Files? ..... 129
9.5 How Do I Enable Logging for Login Failures? ..... 130
9.6 How Do I Scan My Servers? ..... 132
9.7 Why Does Manual Detection Fail? ..... 137
9.8 Does HSS Have a Service Level Agreement? ..... 137
9.9 How Do I Clear an Alarm on Critical File Changes? ..... 137
9.10 Is HSS Available as Offline Software? ..... 137
9.11 Do I Have to Bind an EIP to My Server to Install an HSS Agent on the Server? ..... 137
9.12 Can I Use HSS Via APIs? ..... 137
9.13 Can HSS Alarm Logs Be Stored in OBS? ..... 137
9.14 How Do I Change the Server Bound to an HSS Quota? ..... 138

**A Change History ..... 139**

 Copyright © Huawei Technologies Co., Ltd. 

# 1 About HSS

## 1.1 What Is Host Security Service?

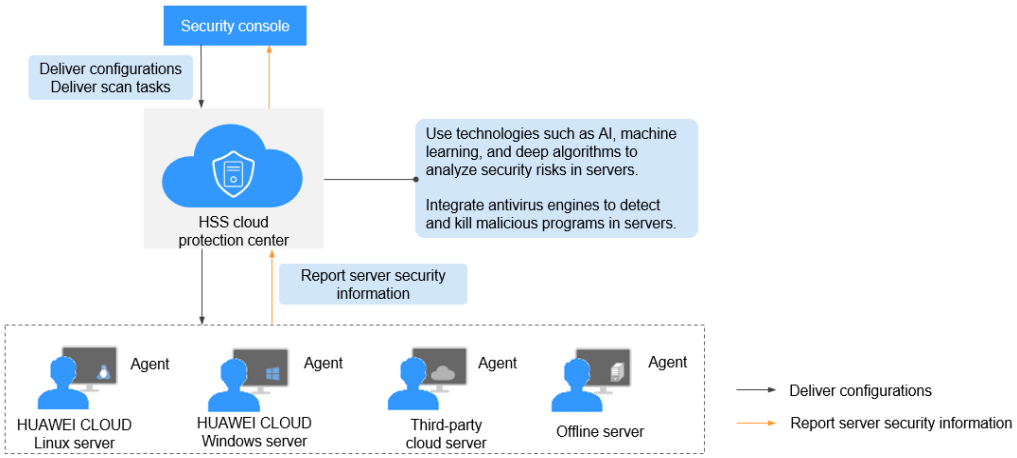
Host Security Service (HSS) helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

### Working Principles

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** illustrates how HSS works.

**Figure 1-1** Working principles




The following table describes HSS components.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 1-1** Components

| Component | Description |
| --- | --- |
| Management console | A visualized management platform, where you can apply configurations in a centralized manner and view the defense status and scan results of servers in a region. |
| HSS cloud protection center | • Uses technologies such as AI, machine learning, and deep algorithms to analyze security risks in servers.<br>• Integrates multiple antivirus engines to detect and kill malicious programs in servers.<br>• Receives configurations and scan tasks sent from the console and forwards them to agents on the servers.<br>• 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 443 is used by default.<br>• 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.<br>• Blocks server attacks based on the security policies you configured.<br>**NOTE**<br>• If the agent is not installed or is abnormal, HSS is unavailable.<br>• An agent can be installed on HUAWEI CLOUD Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), offline servers, and third-party cloud servers.<br>• Select the agent and installation command suitable for your OS.<br>• Web Tamper Protection (WTP) and HSS can use the same agent on a server. |

# 1.2 Where Is HSS Available?

HSS is available in the following regions:

- CN North-Beijing1
- CN North-Beijing4
- CN East-Shanghai1
- CN East-Shanghai2
- CN South-Guangzhou
- CN Southwest-Guiyang1

You can access non-HUAWEI CLOUD servers only in the following regions:

 Copyright © Huawei Technologies Co., Ltd. 

- CN North-Beijing1
- CN East-Shanghai2
- CN South-Guangzhou
- CN North-Beijing4

**Table 1-2** Choosing a region to purchase HSS

| Server | Region HSS Is Purchased for |
| --- | --- |
| ECS<br>BMS<br>HECS | Regions where your ECSs/BMSs/HECSs are deployed |
| Third-party cloud server | Purchase HSS quota in the **CN North-Beijing1**, **CN East-Shanghai2**, **CN South-Guangzhou**, or **CN North-Beijing4** region. To install the HSS agent, perform the installation procedure for non-HUAWEI CLOUD servers. |
| Offline server | |

# 1.3 How Do I Use HSS?

Perform the following steps to get started with HSS:

**Step 1** **Purchase quota.**

Purchase protection quotas in the required edition.

**Step 2** **Install the agent**.

- You can enable HSS only after an HSS agent is installed on the server.
- The basic, enterprise, and WTP editions use the same agent.

**Step 3** (Optional) **Set alarm notifications.**

After alarm notification is 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 the check result** and **handle detected risks**.

**----End**

# 1.4 Can I Upgrade My HSS Edition?

Yes.

 Copyright © Huawei Technologies Co., Ltd. 

### Upgrading Quotas

You can upgrade your basic or enterprise edition HSS quota to the enterprise, premium, or Web Tamper Protection edition as needed.

For more information, see **Upgrading Quota Editions**.

### Switching Editions

You can switch between the editions you purchased.

- If you have purchased quotas in basic, enterprise, and premium editions, you can switch between them.

  Choose **Servers & Quotas** and click the **Servers** tab. In the **Operation** column, click **Enable** and select an edition.

  For details, see "Switching Editions" in **Enabling the Basic/Professional/Premium Edition**.
- To purchase quotas, follow the instructions in **Purchase HSS Quota**.
- To enable WTP for a server that is being protected by basic, enterprise, or premium edition HSS, disable the current edition, and then enable WTP. For details, see **Enabling the WTP Edition**.

  The premium edition is included with WTP and will be enabled if you enable WTP.

## 1.5 Can HSS Protect Local IDC Servers?

Yes, as long as your servers are connected to the Internet.

## 1.6 Does the HSS Agent 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.

## 1.7 What Are the Differences Between HSS, VSS, and WAF?

HSS, Vulnerability Scan Service (VSS), and Web Application Firewall (WAF) are provided by HUAWEI CLOUD to help you defend hosts, websites, and web

 Copyright © Huawei Technologies Co., Ltd. 

applications against risks and threats, improving system security. It is recommended that the services be used together.

**Table 1-3** Differences between HSS, VSS, and WAF

| Service Name | Category | Protected Object | Function |
| --- | --- | --- | --- |
| HSS | Host security | Hosts | • Asset management<br>• Vulnerability management<br>• Intrusion detection<br>• Baseline inspection<br>• Web tamper protection |
| VSS | Application security | Websites | • Vulnerability scan<br>• Web content check<br>• Website health check<br>• Baseline compliance check |
| WAF | Application security | Web applications | • Basic web protection<br>• CC attack protection<br>• Precise protection |

# 1.8 Can HSS Quota Be Shared Between Accounts?

No.

HSS can only be shared by multiple IAM users under the same account, or by an account and its IAM users.

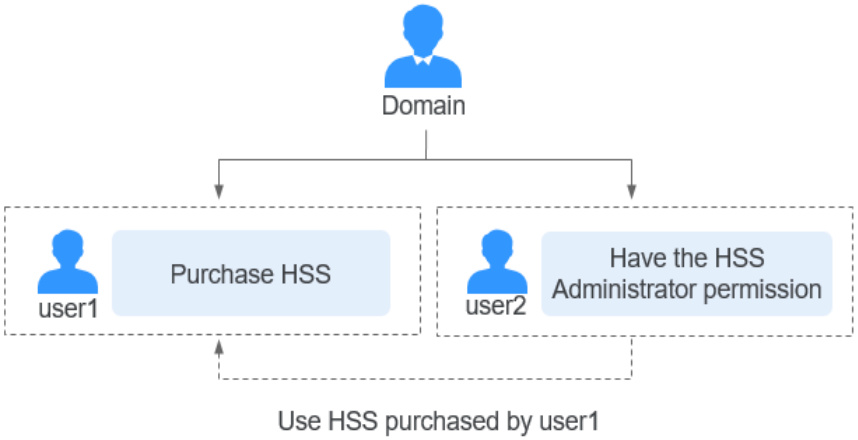
## HSS Shared by Multiple IAM Users Under the Same Account

For example, you have created the account **Domain** and two IAM users **user1** and **user2** under **Domain**.

If **user1** has purchased HSS and **user2** has the HSS Administrator permission, **user2** can also use HSS.


Copyright © Huawei Technologies Co., Ltd.

**Figure 1-2** HSS shared by multiple IAM users under the same account



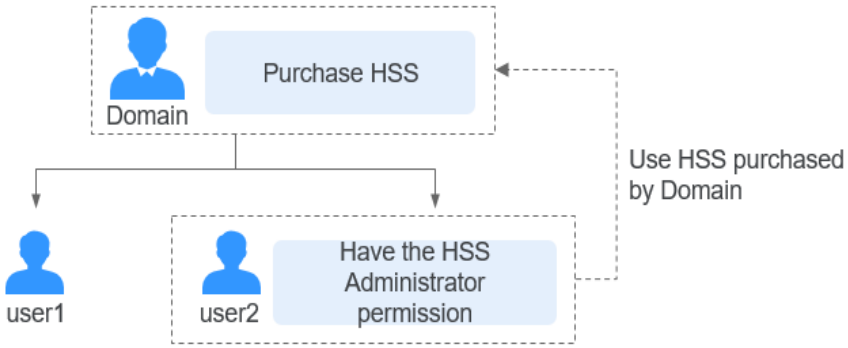

For details about HSS permission management, see **Creating a User and Granting Permissions**.

## HSS Shared Between an Account and IAM Users Under the Account

For example, you have created the account **Domain** and the IAM user **user2** under **Domain**.

- If **Domain** has purchased HSS and **user2** has the HSS Administrator permission, **user2** can also use HSS.

  **Figure 1-3** HSS shared between an account and IAM users under the account (1)

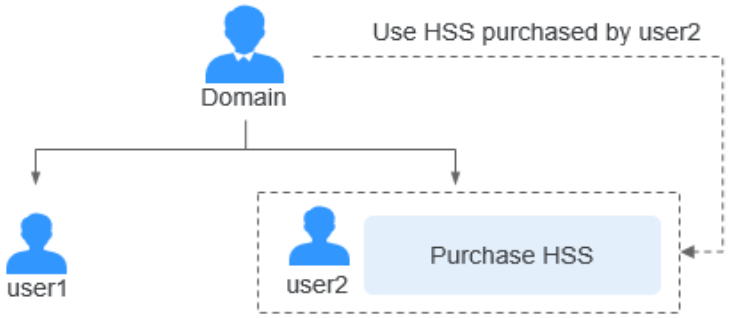
  
  

  For details about HSS permission management, see **Creating a User and Granting Permissions**.

- If **user2** has purchased HSS, **Domain** can also use HSS.


Copyright © Huawei Technologies Co., Ltd.

**Figure 1-4** HSS shared between an account and IAM users under the account (2)




# 1.9 What Is the HSS Agent?

The HSS agent is used to perform scans on all servers, monitor server security status in real time, and reports collected server information 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, monitors server security, and reports collected server information to the cloud protection center.
- The agent blocks server attacks based on the security policies you configured.

NOTE

- If the agent is not installed or is abnormal, HSS is unavailable.
- The agent can be installed on HUAWEI CLOUD Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), Hyper Elastic Cloud Servers (HECSs), offline servers, and third-party cloud servers.
- WTP and HSS can use the same agent on a server.

## Linux Agent Processes

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

The agent contains the following processes:

**Table 1-4** Linux agent processes

| Agent Process Name | Function | Path |
| --- | --- | --- |
| hostguard | Detects security issues, protects the system, and monitors the agent. | /usr/local/hostguard/bin/hostguard |

 Copyright © Huawei Technologies Co., Ltd. 

| Agent Process Name | Function | Path |
| --- | --- | --- |
| 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** Windows agent processes

| Agent Process Name | Function | Path |
| --- | --- | --- |
| HostGuard.exe | Detects and protects the system against security issues. | C:\Program Files (x86)\HostGuard\HostGuard.exe |
| HostWatch.exe | Monitors the agent process. | C:\Program Files (x86)\HostGuard\HostWatch.exe |
| upgrade.exe | Upgrades the agent. | C:\Program Files (x86)\HostGuard\upgrade.exe |

## 1.10 Can HSS Quota Be Shared Across Regions?

No.

If you purchased a quota in a wrong region, unsubscribe from it and purchase a quota in the region of your servers.

## 1.11 Can I Use HSS If My Services Are Not Deployed on HUAWEI CLOUD?

Yes. You can install the agent on HUAWEI CLOUD ECSs, BMSs, offline servers, and third-party cloud servers in the same region to manage them in a unified manner.

For better compatibility and service experience, you are advised to use HUAWEI CLOUD servers.

To make non-HUAWEI CLOUD servers access HUAWEI CLOUD HSS, bind the servers to EIPs and install the agents suitable for their OSs.

### Installing a Linux Agent

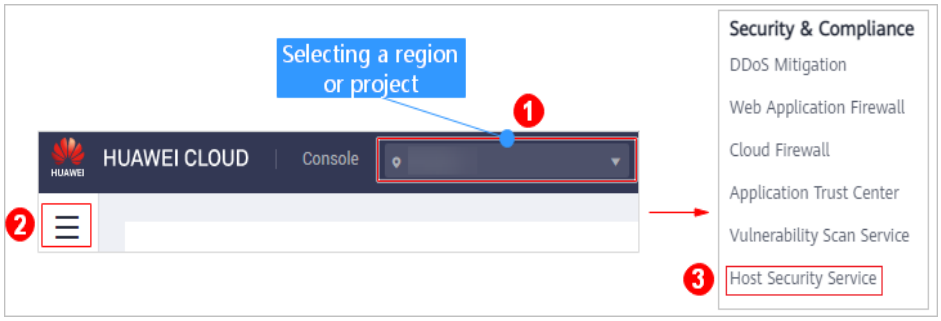
Perform the following steps:

 Copyright © Huawei Technologies Co., Ltd. 

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

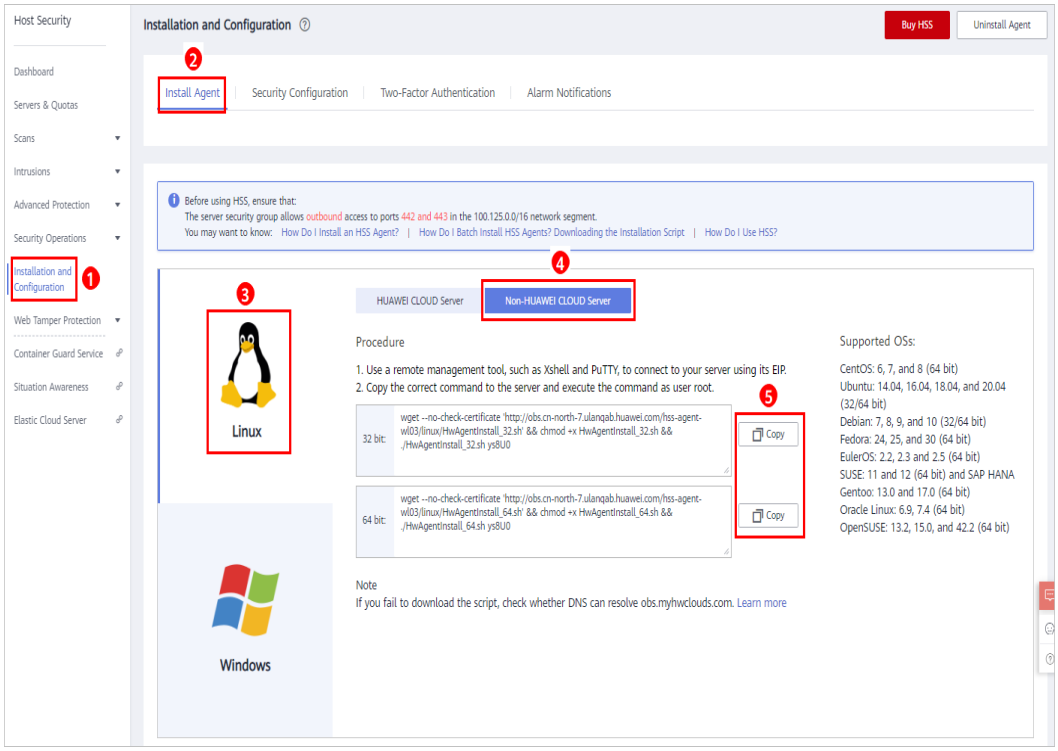
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

**Figure 1-5** Accessing HSS




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

**Figure 1-6** Copying the command for installing the agent




**Step 4** Remotely log in to the server where you plan to install the agent.

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

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

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

 Copyright © Huawei Technologies Co., Ltd. 

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

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

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

```
Hostguard is running
```

**----End**

## Installing a Windows Agent

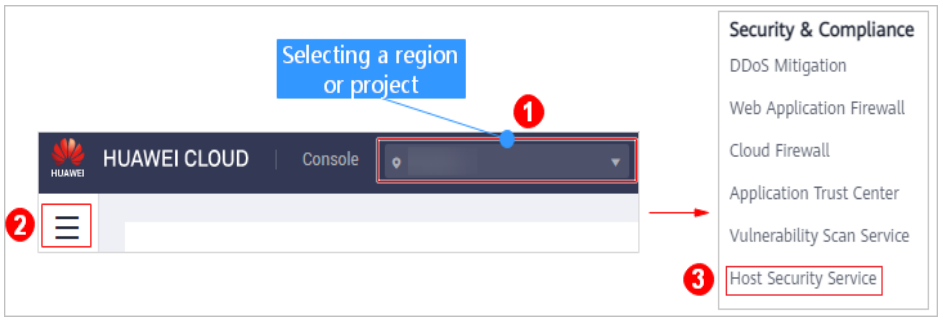
There are two ways to install an agent. This section describes the first one.

- Method 1: Download the agent installation package, upload it to a server, and run the installation command on the server to install the agent.
- Method 2: Log in to a server, log in to the management console from the server, and download and install the agent.

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

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

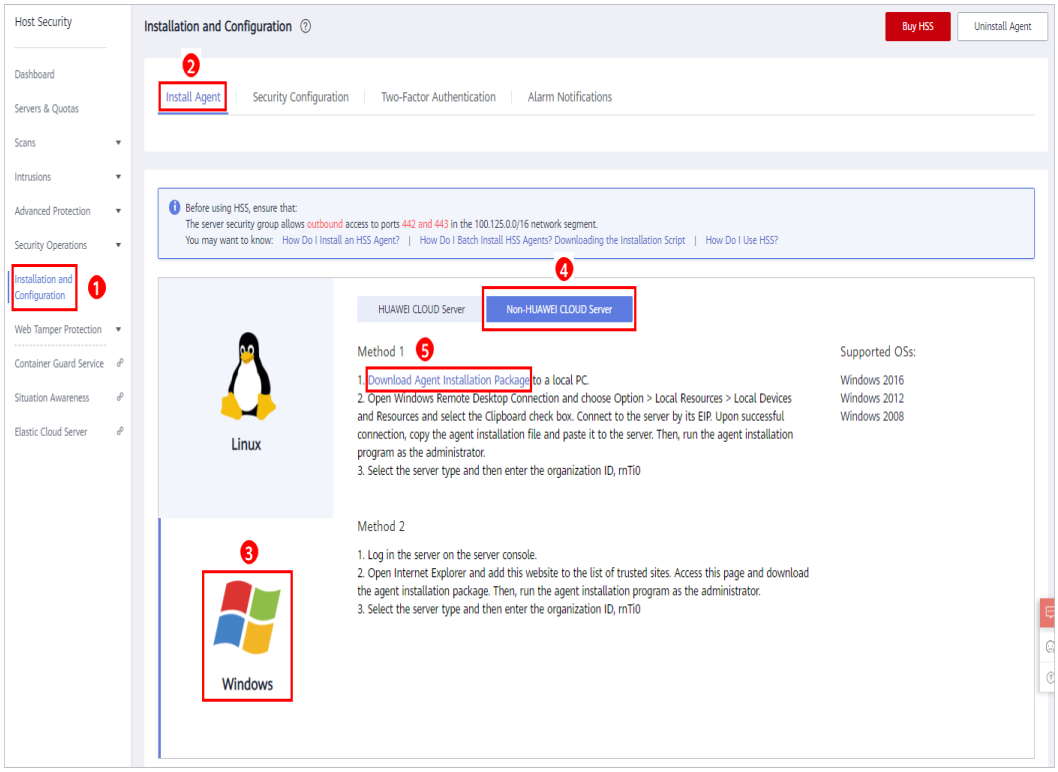
**Figure 1-7** Accessing HSS




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

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 1-8** Installing a Windows Agent




**Step 4** Remotely log in to the server where you plan to install the agent.

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

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

**Step 6** Run the agent installation program as an administrator.

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

Non-HUAWEI CLOUD server: Select **Other Cloud Host**. Copy the value of **Org ID** from the agent installation page, as shown in **Figure 1-9**.

 Copyright © Huawei Technologies Co., Ltd. 

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

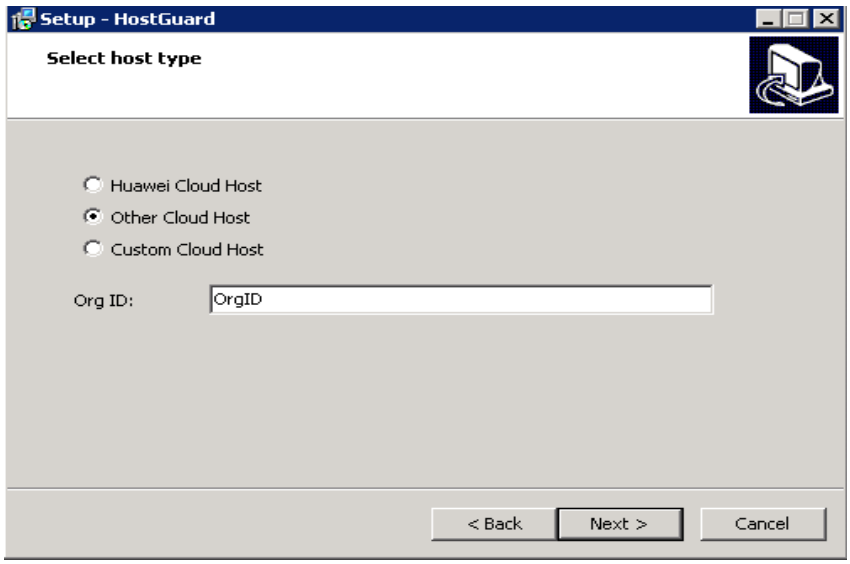
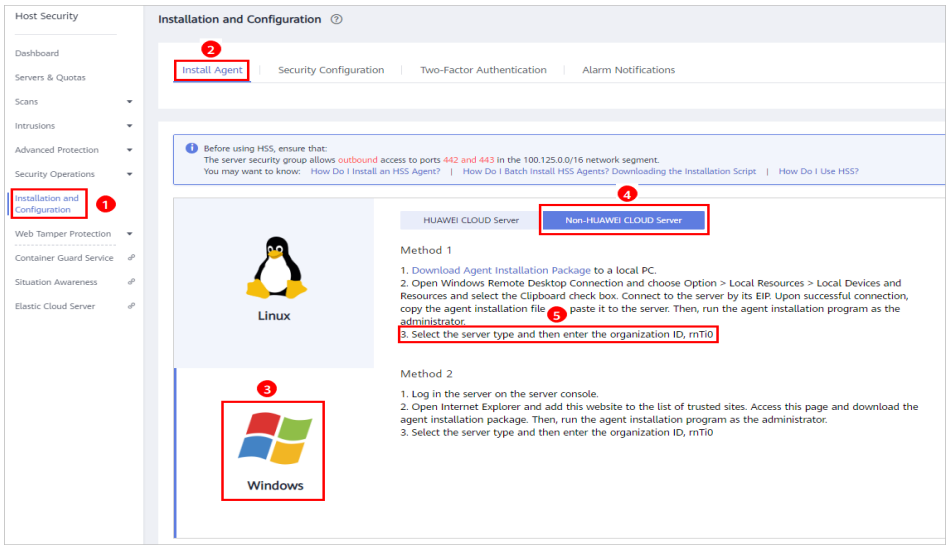



**Figure 1-10** Obtaining an organization ID (for a non-HUAWEI CLOUD server)

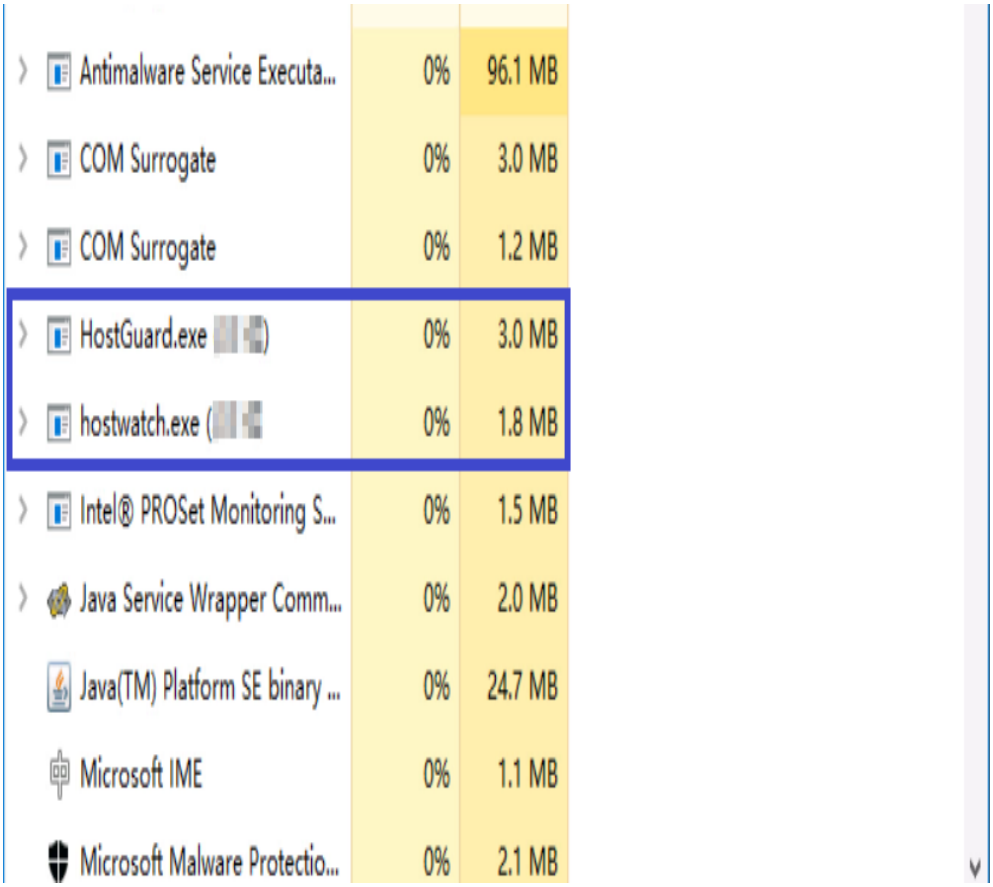



**Step 7** Check the **HostGuard.exe** and **HostWatch.exe** processes in the Windows Task Manager.

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

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 1-11** Checking the agent status




**----End**

# 1.12 Can HSS Protect Offline Servers Using the Same Public IP Address?

No. A server protected by HSS must use a unique public IP address.

# 1.13 What HSS Edition Should I Choose to Earn DJCP L2 Certification?

You need to purchase the enterprise, premium, or WTP edition.

# 1.14 Do I Need to Install Antivirus Software If I Have Enabled HSS?

Yes.

HSS focuses on attack defense and malicious program detection, helping you cope with ransomware attacks before, during, and after an intrusion. For details, see **Ransomware Prevention**.


Copyright © Huawei Technologies Co., Ltd.

You can **create a protection policy**.

You can install antivirus software as a supplement to HSS.

# 1.15 What Are the Differences Between HSS and SA Baseline Checks?

HSS checks your servers for weak password complexity policies and other unsafe settings, and provides **suggestions** for fixing detected risks, helping you reduce security risks and meet security compliance requirements.

Situation Awareness (SA) checks the key configuration items of HUAWEI CLOUD services, generate alarms on unsafe configurations, and provide suggestions for enhancing security.

**Table 1-6** Differences between HSS and SA baseline checks

| Category | HSS | SA |
| --- | --- | --- |
| Object | • HUAWEI CLOUD Elastic Cloud Server (ECS)<br>• Bare Metal Server (BMS)<br>• Hyper Elastic Cloud Server (HECS)<br>• Third-party cloud server<br>• Offline server | • Identity and Access Management (IAM)<br>• Elastic Load Balance (ELB)<br>• Cloud Trace Service (CTS)<br>• Elastic Cloud Server (ECS) |


Copyright © Huawei Technologies Co., Ltd.

| Category | HSS | SA |
| --- | --- | --- |
| Function | • Password complexity policy<br>Check password complexity policies and modify them based on suggestions provided by HSS to improve password security.<br>• Common weak password<br>Change weak passwords to stronger ones based on HSS scan results and suggestions.<br>• Detect unsafe configurations<br>Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS. | • IAM<br>SA checks whether the IAM user is enabled, whether AK/SK authentication, login protection, and operation protection are enabled for IAM users, and whether IAM password policy, IAM login authentication policy, IAM user session timeout policy, and account disabling policy are correctly configured.<br>• Inspection<br>SA checks the ELB health status and whether CTS is enabled.<br>• Infrastructure protection<br>SA checks the configurations of inbound rules, high-risk ports, and remote management ports of security groups, checks whether key pairs are used to log in to ECSs, and checks log metric filtering and alarm event configurations.<br>• Data protection<br>SA checks the ELB certificate validity. |

# 1.16 Can I Add an IP Blacklist in HSS?

HSS has a common IP blacklist to block brute-force attacks, but users cannot modify it.

HSS will block an IP address if it has brute-force attack attempts detected. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.

# 1.17 Do I Need to Enable HSS Again After My Server OS Is Reinstalled?

If you enabled HSS when purchasing ECS or HECS, after your server OS is reinstalled, HSS will automatically install the agent and enable protection.

 Copyright © Huawei Technologies Co., Ltd. 

If you did not enable HSS when purchasing ECS or HECS, after your server OS is reinstalled, you need to **install the agent** on the server and **enable HSS** on the console.

For more information, see **Security Configuration** and **Advanced Protection**.

# 1.18 How Often Does HSS Detect, Isolate, and Kill Malicious Programs?

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, isolate and kill malicious programs (by cloud scan) and abnormal process behaviors. For more information, see **Editions**.
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**.

# 1.19 How Often Are the HSS Virus Database and Vulnerability Database Updated?

The databases are updated in real time.

The HSS vulnerability database is updated immediately when Windows and Linux patches are released.

The virus database is updated immediately when new viruses are detected.

# 1.20 Do I Have to Deploy HSS on All My Cloud Servers?

You are advised to deploy HSS on all your cloud servers.

If HSS is deployed on all your servers, and a virus infects one of them, the virus will not be able to spread to others and damage your entire network.

For details about HSS capabilities, see **Editions**.

For details about how to purchase HSS, see **Purchase HSS Quota**.


Copyright © Huawei Technologies Co., Ltd.

# 1.21 How Do I Enable the HSS Basic Edition Free of Charge?

NOTE

1. The HSS basic edition is available for free.
2. If you use the basic edition charged in yearly/monthly mode, it will be automatically switched to the pay-per-use mode after it expires, and will still be free of charge. For more information, see **Editions**.
3. If you attempt to enable the basic edition in yearly/monthly mode, a message indicating insufficient quota may be displayed. In this case, select the basic edition in pay-per-use mode.
4. The basic edition is free of charge and does not have a validity period limit.

## Enabling Basic Edition HSS

| Scenario | Where to Enable | Enabling Mode | Procedure | How to Check |
| --- | --- | --- | --- | --- |
| Enable protection for ECS or HECS. | (Recommended) Enable this function when purchasing ECS or HECS on the console. | Automatic | • When you purchase an ECS, select **Enable** for the **Host Security** parameter and select the basic edition. HSS will automatically install the agent on the ECS and enable the basic edition in pay-per-use mode.<br>For more information, see **Configuring Basic Settings** and **Enabling HSS**.<br>• When you purchase an HECS, select the HSS basic edition. HSS will automatically install the agent for HECS and enable the basic edition (pay-per-use).<br>For more information, see **Configuring Basic Settings** and **Enabling HSS**. | You can check the protection status in the **server list**. |

 Copyright © Huawei Technologies Co., Ltd. 

| Scenario | Where to Enable | Enabling Mode | Procedure | How to Check |
| --- | --- | --- | --- | --- |
| Enable HSS for existing servers. | Enable this function on the HSS console. | Manual | On the HSS console, manually install the HSS agent and enable the basic edition.<br>1. Install the **Linux** or **Windows** agent.<br>2. **Enable HSS**.<br>To enable alarm notifications, see **Enabling Alarm Notification**. | |

For more information, see **HSS basic edition (free)**.

# 1.22 How Does HSS Transfer Data?

HSS servers use port 443, and HSS agents use random ports for communication. Agents can transfer data from any port to port 443 of HSS servers.

HSS transfers data via IP. Agents transmit data via DNS. No data is lost during the transmission.


Copyright © Huawei Technologies Co., Ltd.

# 2 HSS Purchase

## 2.1 How Can I Use the Free HSS Included with ECS?

### Enabling HSS While Purchasing an ECS

- When purchasing a HUAWEI CLOUD ECS, you can enable basic or enterprise edition HSS. HSS will install its agent on the ECS and protect the ECS.

  For more information, see **Table 2-1**.

  **Table 2-1** Purchase parameters

  | ECS Billing | HSS Edition | Enable HSS | HSS Billing |
  | --- | --- | --- | --- |
  | Yearly / Monthly | Basic | Basic (pay-per-use) | Free |
  | Pay-per-use | Basic or Enterprise | Basic (pay-per-use) or Enterprise (pay-per-use) | • Basic (pay-per-use): free<br>• Enterprise (pay-per-use): You will be charged based on usage duration. |

  Currently, this feature is available only in **CN North-Beijing1**, **CN North-Beijing4**, **CN East-Shanghai1**, **CN East-Shanghai2**, **CN South-Guangzhou**, and **CN Southwest-Guiyang1**.

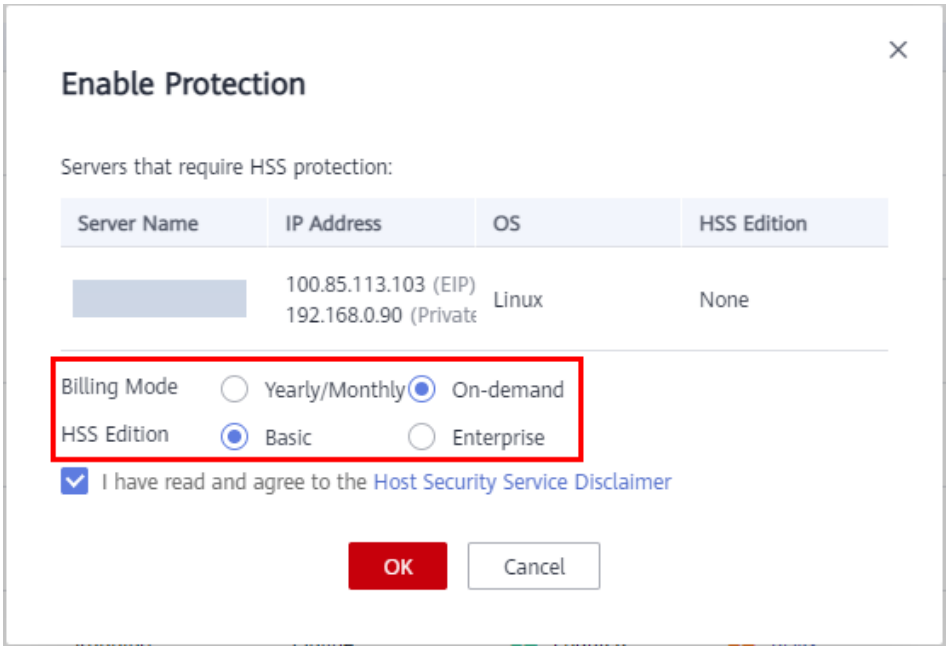
- You can also purchase **editions** other than the basic and enterprise editions. To **enable higher editions**, disable the Basic (pay-per-use) or Enterprise (pay-per-use) edition first.

 Copyright © Huawei Technologies Co., Ltd. 

### Enabling HSS for an Existing ECS

- Install the HSS agent on the ECS and manually enable the Basic (pay-per-use) edition. You can use the basic edition free of charge.

  **Figure 2-1** Enabling Basic (pay-per-use) edition




- You can also purchase **editions** other than the basic and enterprise editions. To **enable higher editions**, disable the Basic (pay-per-use) edition first.

# 2.2 Why Can't I Select Free HSS When Purchasing ECS?

Your ECS OS version is probably not supported by HSS.

This topic lists the OS versions supported by HSS.

**NOTICE**

The agent is probably incompatible with the Linux or Windows OS 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 2-2** and **Table 2-3** list Linux OS versions supported by HSS.

  **Table 2-2** Linux OS version (x86 computing)

| No. | OS Version |
| --- | --- |
| 1 | CentOS: 6, 7, and 8 (64 bit) |
| 2 | Debian: 7, 8, 9, and 10 (32/64 bit) |
| 3 | EulerOS: 2.2, 2.3, and 2.5 (64 bit) |


Copyright © Huawei Technologies Co., Ltd.

| No. | OS Version |
| --- | --- |
| 4 | Fedora: 24, 25, and 30 (64 bit) |
| 5 | OpenSUSE: 13.2, 15.0, and 42.2 (64 bit) |
| 6 | Ubuntu: 14.04, 16.04, 18.04, and 20.04 (32/64 bit) |
| 7 | Gentoo: 13.0 and 17.0 (64 bit) |
| 8 | Oracle Linux: 6.9 and 7.4 (64 bit) |

**Table 2-3** Linux OS version (Kunpeng computing)

| No. | OS Version |
| --- | --- |
| 1 | CentOS: 7.4, 7.5, 7.6, and 8.0 64-bit with ARM (40 GB) |
| 2 | EulerOS: 2.8 64-bit with ARM (40 GB) |
| 3 | Fedora: 29 64-bit with ARM (40 GB) |
| 4 | OpenSUSE: 15.0 64-bit with ARM (40 GB) |
| 5 | Ubuntu: 18.04 64-bit with ARM (40 GB) |

- Table 2-4 lists Windows OS versions supported by HSS.

**Table 2-4** Supported Windows OSs

| No. | OS Version | Constraint |
| --- | --- | --- |
| 1 | Windows Server 2019 Datacenter 64-bit English (40 GB) | If a piece of third-party security software, such as McAfee, has been installed on your server, stop the protection function on the software before installing an HSS agent. After you install the agent, you can re-enable the protection function on the software. |
| 2 | Windows Server 2019 Datacenter 64-bit Chinese (40 GB) | |
| 3 | Windows Server 2016 Standard 64-bit English (40 GB) | |
| 4 | Windows Server 2016 Standard 64-bit Chinese (40 GB) | |
| 5 | Windows Server 2016 Datacenter 64-bit English (40 GB) | |
| 6 | Windows Server 2016 Datacenter 64-bit Chinese (40 GB) | |
| 7 | Windows Server 2012 R2 Standard 64-bit English (40 GB) | |
| 8 | Windows Server 2012 R2 Standard 64-bit Chinese (40 GB) | |


Copyright © Huawei Technologies Co., Ltd.

| No. | OS Version | Constraint |
| --- | --- | --- |
| 9 | Windows Server 2012 R2 Datacenter 64-bit English (40 GB) | |
| 10 | Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB) | |

# 2.3 How Do I Purchase and Enable HSS?

## Purchasing HSS in Pay-per-use Mode

Log in to the HSS console and choose **Servers & Quotas**. In the server list, click **Enable** in the row of a server. In the **Enable Protection** dialog box, set **Billing Mode** to **On-demand**, select an edition, and click **OK** to **enable protection**.

## Purchasing HSS in Yearly/Monthly Mode

**Purchase HSS** on the console. Log in to the HSS console and choose **Servers & Quotas**. In the server list, click **Enable** in the row of a server. In the **Enable Protection** dialog box, set **Billing Mode** to **Yearly/Monthly**, select an edition, and click **OK** to **enable protection**. If the current edition does not meet your service requirements, you can **switch to another edition**.

NOTE

Basic edition HSS is provided for free when you purchase ECS or HECS and will not expire.


Copyright © Huawei Technologies Co., Ltd.

# 3 Deployment and Configuration

## 3.1 Agent

### 3.1.1 Do I Need to Install the HSS Agent After Purchasing HSS?

#### Enabling HSS When Purchasing ECS

When purchasing a HUAWEI CLOUD ECS, you can enable basic or enterprise edition HSS. HSS will install its agent on the ECS and protect the ECS.

- If you set **Billing Mode** to **Yearly/Monthly**, you can only enable basic edition HSS, which is free of charge. For more information, see **How Can I Use the Free HSS Included with ECS?**.
- If you set **Billing Mode** to **Pay-per-use**, you can enable the basic or enterprise edition.

Currently, this feature is available only in **CN North-Beijing1**, **CN North-Beijing4**, **CN East-Shanghai1**, **CN East-Shanghai2**, **CN South-Guangzhou**, and **CN Southwest-Guiyang1**.

You can also purchase **editions** other than the basic and enterprise editions. You do not need to install the agent again. For details about the differences between them, see **Editions**.

#### Other Scenarios

The agent will not be automatically installed in other scenarios. You need to manually **install the agent** and **enable protection**.

### 3.1.2 How Do I Install the Agent?

- HUAWEI CLOUD server
  - For details about how to install the Linux agent, see **Installing an Agent on a HUAWEI CLOUD Server Running Linux**.

 Copyright © Huawei Technologies Co., Ltd. 

  - For details about how to install the Windows agent, see **Installing an Agent on HUAWEI CLOUD Server Running Windows**.
- Non-HUAWEI CLOUD server
  - For details about how to install the Linux agent, see **Installing an Agent on a HUAWEI CLOUD Server Running Linux**.
  - For details about how to install the Windows agent, see **Installing an Agent on HUAWEI CLOUD Server Running Windows**.

### Helpful Links

- **What Do I Do If Agent Installation Fails?**
- **How Do I Fix an Abnormal Agent?**
- **How Do I Uninstall the Agent?**

## 3.1.3 How Do I Install the Agent on Servers in Batches?

### Windows OS

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

**Step 1** Purchase a HUAWEI CLOUD ECS and select the required Windows OS image. For details, see **Purchasing an ECS**.

**Step 2** Install the HSS agent on the purchased ECS. For details, see **Installing an Agent on a HUAWEI CLOUD Server Running Windows**.

NOTE

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

**Step 3** Stop the HostGuard process in the Windows Task Manager.

**Step 4** Delete the files in **C:\Program Files(x86)\HostGuard\config\agentinfo**.

**Step 5** 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 **Step 3** and **Step 4** again.

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

**----End**

### Linux OS

Install Linux agents in batches in either of the following ways:

**Method 1: Installing agents in batches using scripts**

**Prerequisites**

Prepare a Linux computer used for running the batch installation script.

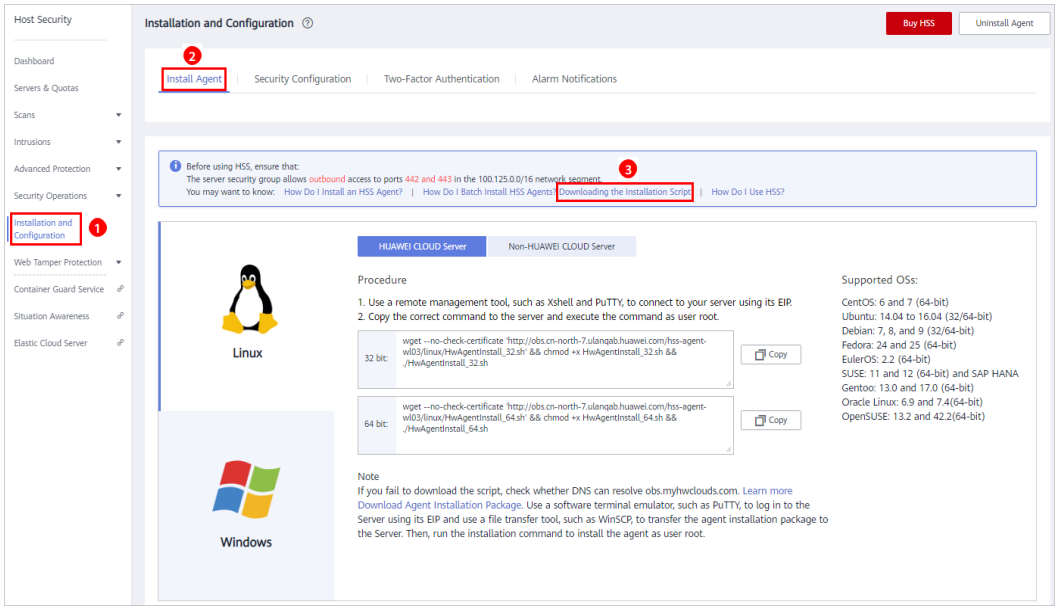
 Copyright © Huawei Technologies Co., Ltd. 

- Log in to the Linux computer and the target servers with the same user.
- Exchange data between the Linux computer and the target servers via SSH without requiring passwords.
- Configure the Linux computer to ignore SSH login authentication.

**Procedure**

**Step 1** Download the batch installation script, as shown in **Figure 3-1**.

**Figure 3-1** Downloading the installation script




**Step 2** Collect the IP addresses, SSH username and password, and passwords of the **root** user for logging in to the target servers.

**Step 3** Save the IP addresses, SSH username and password, and passwords of the **root** user in a text file **hostinfo.txt** (UTF-8) in sequence and separate them with spaces. A single record occupies a line, terminated by a line feed. The file format is Unix (can be edited using notepad++).

For example, there are two servers. The IP address, SSH username, and password of the **root** user for logging in to server A is 192.168.1.101, **root**, and 123456, separately. The IP address, SSH username and password, and password of the **root** user for logging in to server B is 192.168.1.102, **test**, test123, and 123456 (see **Figure 3-2**).

**Figure 3-2** Example

```
1  192.168.1.101 root 123456 123456
2  192.168.1.102 test test123 123456
3
```

**Step 4** Use a Linux computer (4 vCPUs, 8 GB is recommended) to run the script. This computer must be able to connect to the target servers via SSH (port 22).

**Step 5** Check whether Ansible is installed on the Linux computer. If no, install Ansible.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 6** Upload the host configuration file **hostinfo.txt** and the agent installation script (**deploy-ansible-expect**) to the same directory on the Linux computer.

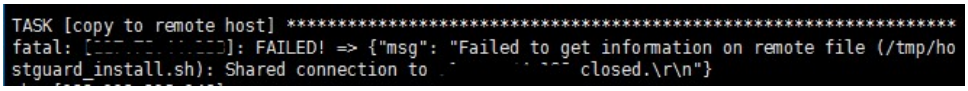
**Step 7** Run the **sh config.sh hostinfo.txt** command to generate the configuration file **hosts** required by Ansible.

**Step 8** Run the **chmod u+x install.sh; ./install.sh** command to complete the batch installation.

**----End**

NOTE

1. When you execute the Ansible script, the **su** command is executed by default to switch to the **root** user. However, on some ECSs, running the **su** command cannot switch to the **root** user. If the operation fails due to insufficient permission, modify **ansible_become_method=su** in the **hosts** file in the installation script to **ansible_become_method=sudo**, save the file, and run the **install.sh** script again.
2. The error message shown in the following figure may be displayed when Ansible is used to install HSS agents on some ECSs (the error was found on ubuntu16). That is because the default python is not configured on the target ECSs. You can use either of the following methods to remove this error:




   1. Follow the steps as instructed in **How Do I Install an HSS Agent?** to install an HSS agent.
   2. Log in to the required server and set the default Python.

      You can run **sudo update-alternatives --install /usr/bin/python python /usr/bin/python3 10**.

      Alternatively, you can run **ln -s /usr/bin/python3 /usr/bin/python(ln -s /usr/bin/python2 /usr/bin/python)**.

### Method 2: Installing agents in batches using an image

**Step 1** Purchase a HUAWEI CLOUD ECS and select the required Linux OS image. For details, see **Purchasing an ECS**.

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

NOTE

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

**Step 3** 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 4** Delete the configuration file.

Run the **rm -rf** command to delete the files in the **/usr/local/hostguard/conf/agentinfo** directory in the Linux OS.

**Step 5** Stop the ECS and use it to create an image. For details, see **Creating an Image**.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

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

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

**----End**

# 3.1.4 How Do I Install the Agent from the Command Line (on Windows)?

## Prerequisites

- The online server where the agent is to be installed must be able to communicate with the network segment. The security group of your server must allow outbound access to ports 442 and 443 on the 100.125.0.0/16 network segment.

## Procedure

**Step 1** Log in to the Windows ECS as an administrator.

**Step 2** Open a browser, and enter the address of the Agent installation package in the address box to download and decompress the installation package.

**Table 3-1** Package download paths

| Name | Format | Path |
| --- | --- | --- |
| Agent installation package for Windows | zip | CN North-Beijing1: **https://hostguard-agent.obs.cn-north-1.myhuaweicloud.com/windows/HSS-WindowsAgentSetup_x86.zip**<br>CN North-Beijing4: **https://hss-agent-bj04.obs.cn-north-4.myhuaweicloud.com/windows/HSS-WindowsAgentSetup_x86.zip**<br>CN East-Shanghai1: **https://obs.cn-east-3.myhuaweicloud.com/hss-agent-sh01/windows/HSS-WindowsAgentSetup_x86.zip**<br>CN East-Shanghai2: **https://hss-agent-sh02.obs.cn-east-2.myhuaweicloud.com/windows/HSS-WindowsAgentSetup_x86.zip**<br>CN South-Guangzhou: **https://hss-agent-gz01.obs.cn-south-1.myhuaweicloud.com/windows/HSS-WindowsAgentSetup_x86.zip**<br>CN Southwest-Guiyang1: **https://obs.cn-southwest-2.myhuaweicloud.com/hss-agent-gy01/windows/HSS-WindowsAgentSetup_x86.zip** |

**Step 3** Inside the search field from your taskbar, enter **cmd** to open the **Command Prompt** window. Go to the agent installation path.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 4** Run the **.\hostguard_setup.exe /silent** command to install the agent.

After the agent is installed, you are advised to delete the agent installation package.

**----End**

## 3.1.5 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 host is identified as an attack IP address but cannot be unblocked.
- Cause: HSS and DenyHosts both block possible attack IP addresses, but HSS cannot unblock the IP addresses that were blocked by DenyHosts.
- Handling method: Stop DenyHosts.

1. Log in as user **root** to ECS.
2. 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
   ```

3. Run the following command to stop DenyHosts:

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

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

   **chkconfig --del denyhosts;**

## 3.1.6 What Is the Default Agent Installation Path?

The agent installation paths on servers running the Linux or Windows OS cannot be customized. **Table 3-2** describes the default paths.

**Table 3-2** Default agent installation paths

| OS | Default Installation Path |
| --- | --- |
| Linux | /usr/local/hostguard/ |
| Windows | C:\Program Files (x86)\HostGuard |

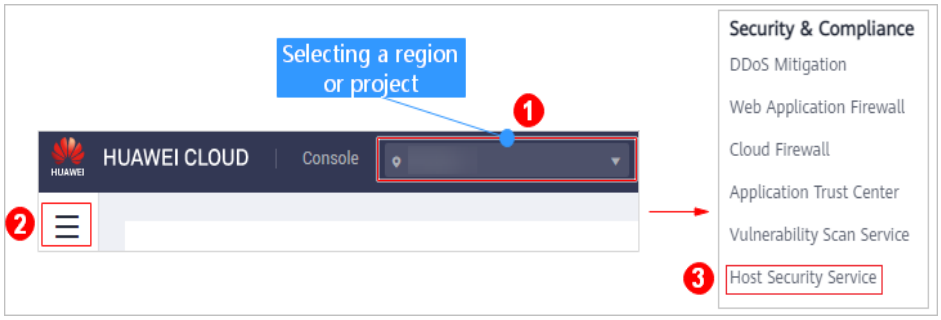
## 3.1.7 How Do I Filter Servers Where No Agents Have Been Installed?

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

 Copyright © Huawei Technologies Co., Ltd. 

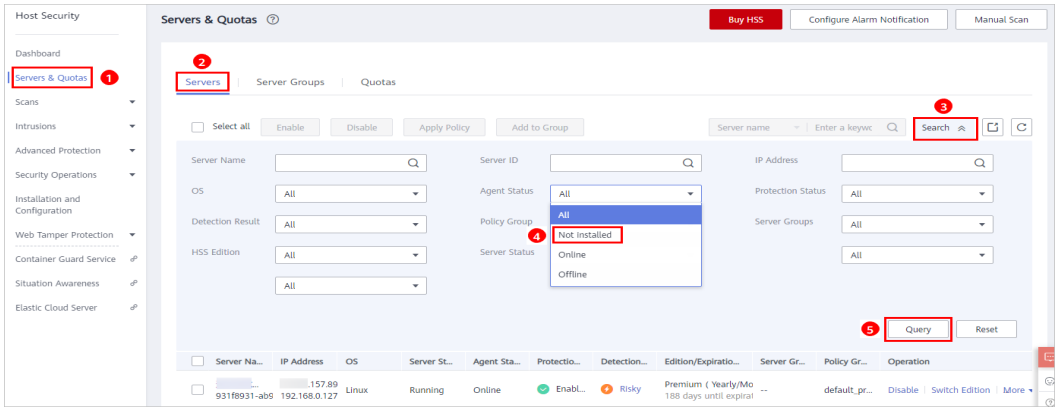
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

**Figure 3-3** Accessing HSS




**Step 3** On the **Servers** page, filter the servers where no agents have been installed, as shown in **Figure 3-4**.

**Figure 3-4** Filtering the servers where no agents have been installed




Possible agent statuses are:

- **Not installed**: The agent has not been installed or successfully started.
- **Online**: The agent is running properly.
- **Offline**: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers.

  You can click **Offline**, and view servers whose agents are offline and the offline reasons at the bottom of the page that is displayed.

**----End**

# 3.1.8 What Do I Do If Agent Installation Fails?

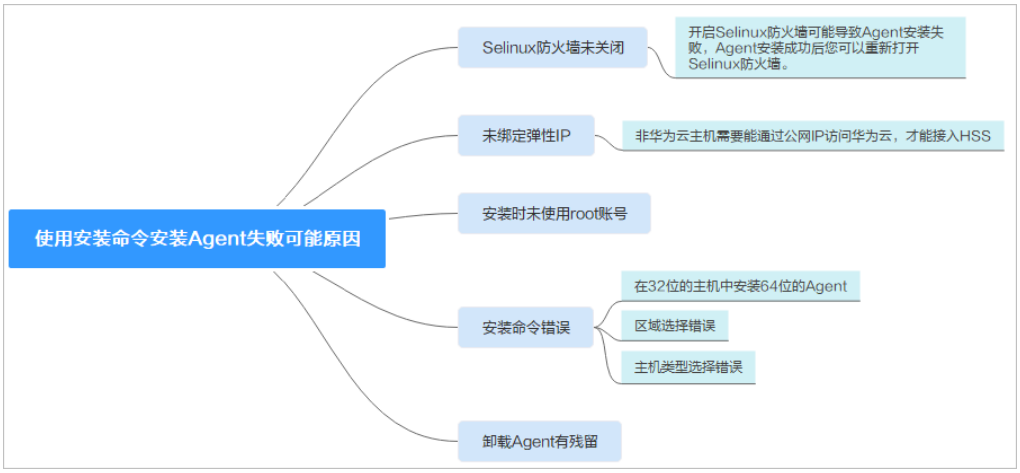
## Failed to Install the Agent by Running the Installation Commands

### Symptom

The agent fails to be installed by running commands. The server list page on the console still indicates that the agent is not installed.

 Copyright © Huawei Technologies Co., Ltd. 

### Possible Causes




### Solution

**Step 1** Check whether the SELinux firewall of the server is disabled.

- If it is, go to **Step 2**.
- If it is not, disable it and install the agent again.

**Step 2** Check whether there is an EIP bound to the server.

- If it has, go to **Step 3**.
- If there is not, bind an EIP to the server and reinstall the agent.

**Step 3** Check whether the installation command is suitable for the server region and OS.

1. Switch to the server region. For details, see **Switching a Region**.
2. Copy the installation commands suitable for your server OS.
   - Run 32-bit installation commands on a 32-bit server.
   - Run 64-bit installation commands on a 64-bit server.

- If it has, go to **Step 4**.
- If the commands you used are incorrect, install the agent again with correct ones.

**Step 4** Check whether the installation was performed by user **root**.

- If it has, go to **Step 5**.
- If it was not, install the agent again as user **root**.

**Step 5** **Uninstall the agent** as user **root** and forcibly install it.

- If the installation is successful, no further action is required.
- If the installation fails, contact technical support.

**----End**

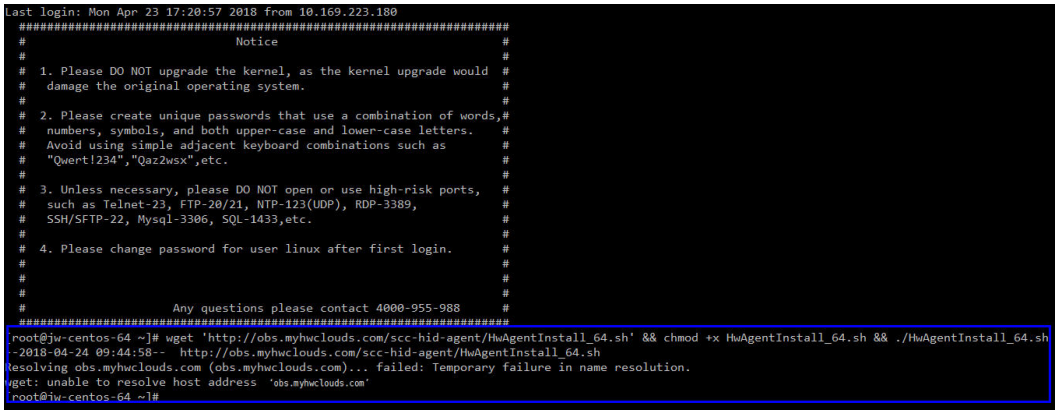
## Failed to Install the Agent by Running the Script

### Symptom

An error is reported during the agent installation. The following error message is displayed when the agent is being installed by using a script:

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-5** Error message




### Possible Causes

The DNS address is incorrectly configured. The domain name **obs.myhuaweicloud.com** cannot be resolved.

### Solution

Perform the following steps to correctly configure DNS and retry installation:

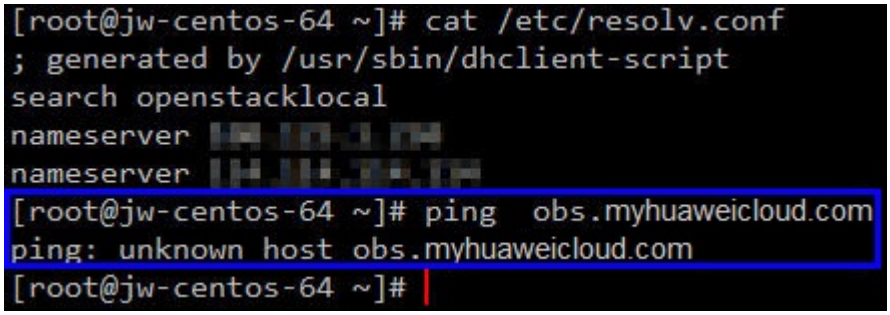
**Step 1** Run the **cat /etc/resolv.conf** command to view the **resolv.conf** file.

**cat /etc/resolv.conf**

**Step 2** Run the **ping** *Domain_name* command. If the command output in **Figure 3-6** is displayed, go to **Step 3**.

**ping obs.myhuaweicloud.com**

**Figure 3-6** Failing to ping the domain name




**Step 3** Run the following command to open the **resolv.conf** file:

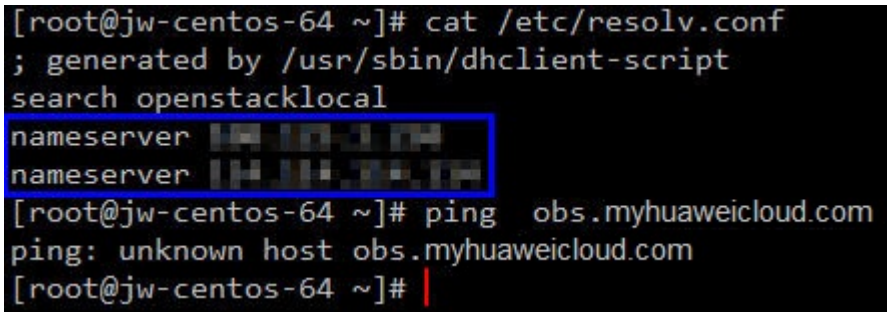
**vi /etc/resolv.conf**

Replace the IP addresses highlighted in **Figure 3-7** with common DNS IP addresses.

```
nameserver Common_DNS_IP_address_1
nameserver Common_DNS_IP_address_2
```

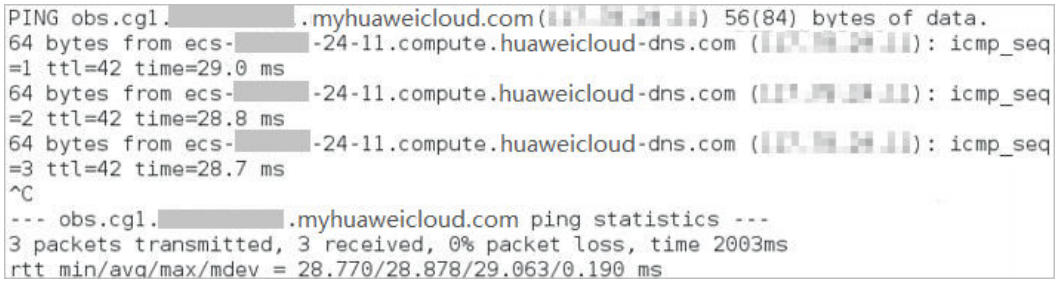
 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-7** The part to be replaced




**Step 4** After the modification, run the **ping obs.myhuaweicloud.com** command again. If information similar to the following is displayed, the domain name is pinged successfully.

**Figure 3-8** Message indicating the domain name can be pinged




**Step 5** Run the installation script.

**----End**

## Example of Agent Installation Troubleshooting

- Failure information: install rpm package failed.

  Possible cause: The wrong installation package was used.

  Solution:

  a. Uninstall the agent. For details, see **How Do I Uninstall the Agent?**

  b. Reinstall the agent by referring to **Installing an Agent on the Linux OS** or **Installing an Agent on the Windows OS**.

# 3.1.9 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:

- **Not installed**: 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.


Copyright © Huawei Technologies Co., Ltd.

## Possible Causes

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

## Solution

**Step 1** Fix network problems (if any).

Ensure that the outbound configurations of the security group of your server allow access to port 443 in the 100.125.0.0/16 network segment.

After the network recovers,

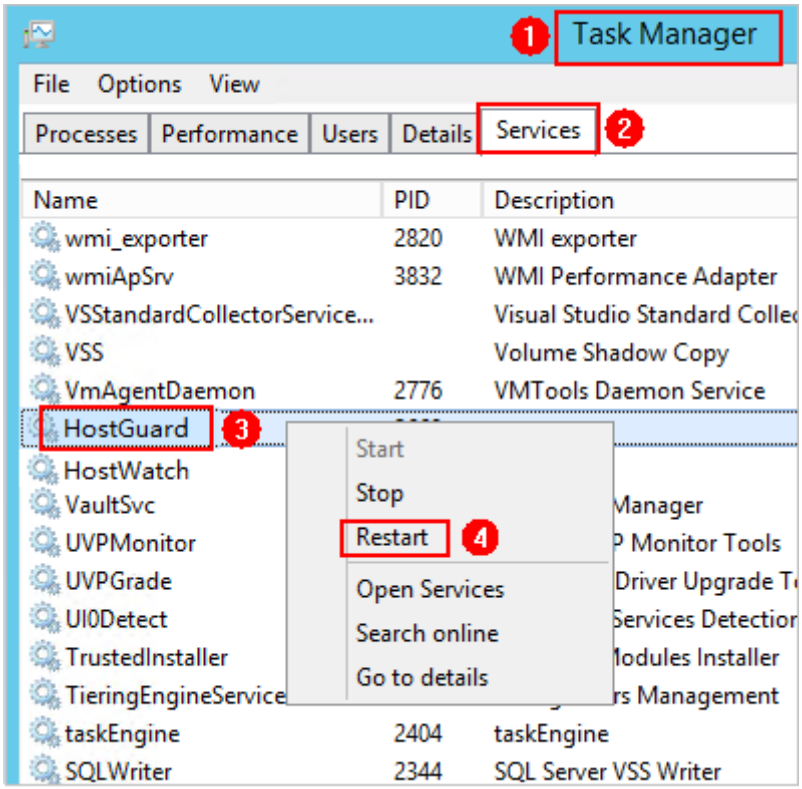
- If the agent status is **Online**, no further action is required.
- If the agent status is **Not installed** or **Offline**, go to **Step 2**.

**Step 2** Log in to the server and restart the agent. The agent status **Not installed** or **Offline** indicates that the agent process is probably abnormal.

- Windows OS

  Log in to the server as **administrator** and restart the client.

  **Figure 3-9** Restarting Windows agent




- Linux OS

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

 Copyright © Huawei Technologies Co., Ltd. 

**service hostguard restart**

If the following information is displayed, the restart is successful: If no command output is displayed, **uninstall the agent** and then **install it**.

```
root@HSS-Ubuntu32:~#service 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**

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

- CPU usage is automatically controlled within 10%. If the CPU usage exceeds 10%, the agent will automatically reduce CPU usage, spending more time on scans. This does not affect scan results.
- The memory usage is controlled within 150 MB. If the memory usage exceeds 200 MB, the agent automatically restarts within 5 minutes.

## 3.1.11 Does HSS Agent Installation Affect My Services?

Installing HSS agent does not affect online services or servers.

The HSS agent is used to perform scans on all servers, monitor server security status in real time, and reports collected server information to the cloud protection center.

For more information, see **What Is the HSS Agent?**.

## 3.1.12 Do WTP and HSS Use the Same Agent?

Yes.

You only need to install one agent on a server to use both services.

## 3.1.13 How Do I Uninstall the Agent?

### 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.

### Prerequisites

- Login credentials have been obtained.


Copyright © Huawei Technologies Co., Ltd.

- **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.

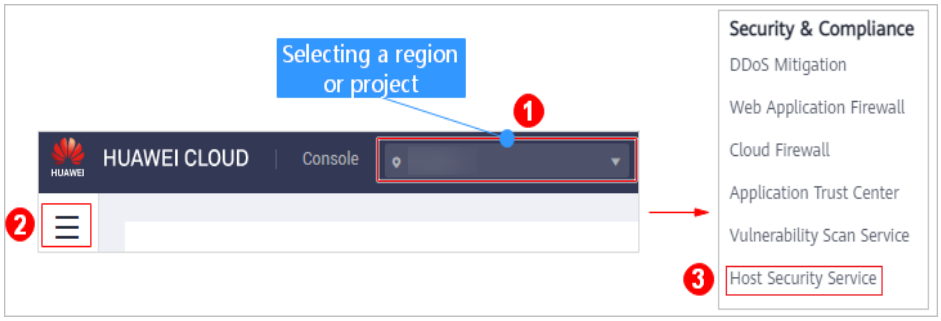
NOTE

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** > **Host Security Service**.

**Figure 3-10** Accessing HSS

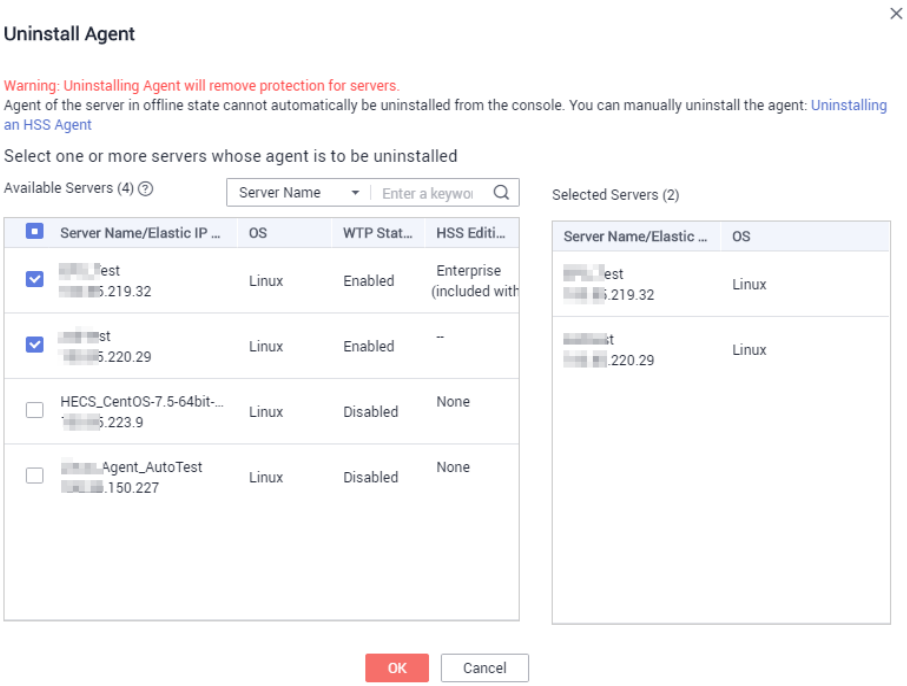



**Step 3** In the navigation pane, choose **Security Operations** > **Installation and Configuration**. In the upper right corner of the **Installation and Configuration** page, click **Uninstall Agent**.

**Step 4** On the **Uninstall Agent** page, select the server whose agent is to be uninstalled.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-11** Uninstalling an agent




**Step 5** Click **OK**.

In the server list, if **Agent Status** of the server is **Offline**, its agent is successfully uninstalled.

**----End**

## Uninstalling the Agent from the Server

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

NOTE

After the agent is uninstalled from a 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. Then run the **su - root** command to switch to user **root**.
  b. In any directory, run the following command to uninstall the agent:
     i. If the agent was installed using an .rpm package, run the **rpm -e --nodeps hostguard** command.
     ii. If the agent was installed using a .deb package, run the **dpkg -P hostguard** command.

     If the following information is displayed, the agent is uninstalled:

```
Stopping Hostguard...
Hostguard stopped
Hostguard uninstalled.
```

 Copyright © Huawei Technologies Co., Ltd. 

- **Uninstalling the Windows agent**
  a. Log in to the server from which you want to uninstall an HSS agent.
  b. Click **Start** and choose **Control Panel** > **Programs**. Then select **HostGuard** and click **Uninstall**.

     NOTE

     - Alternatively, go to the installation directory and double-click **unins000.exe**.
     - If you have created a folder for storing the agent shortcut under the **Start** menu when installing the agent, you can also choose **Start** > **HostGuard** > **Uninstall HostGuard** to uninstall HostGuard.

  c. In the **Uninstall HostGuard** dialog box, click **Yes**.
  d. After the uninstallation is complete, click **OK**.

# 3.2 Security Configurations

## 3.2.1 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.

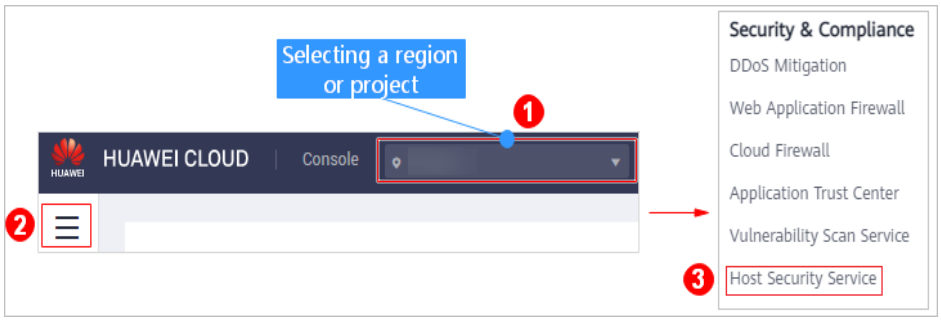
### Normal or Expired

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 & Compliance** > **Host Security Service**.

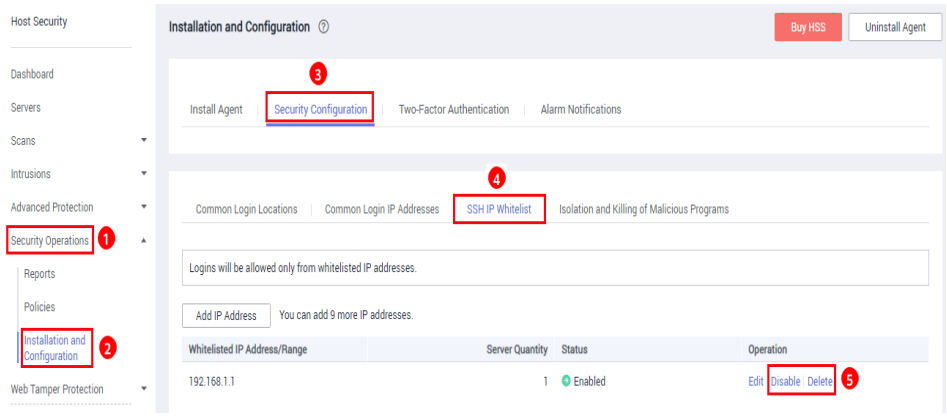
**Figure 3-12** Accessing HSS




**Step 3** On the **Installation and Configuration** page, click **Security Configuration**, and click **SSH IP Whitelist**.


Copyright © Huawei Technologies Co., Ltd.

**Figure 3-13** SSH login IP address whitelist




**Step 4** Click **Disable** or **Delete** to clear the whitelist.

**----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.

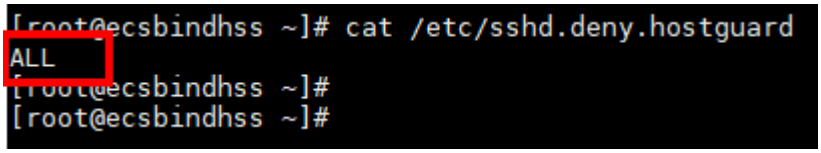
Perform the following steps to clear the configured SSH login IP address whitelist:

**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 3-14**.

**cat /etc/sshd.deny.hostguard**

**Figure 3-14** 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**

 Copyright © Huawei Technologies Co., Ltd. 

## 3.2.2 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 HUAWEI CLOUD 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 your login IP address was blocked as an attack source, go to the **Events** page, click **Blocked IP Addresses**, and unblock your 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 blocked for this reason, add the IP address to whitelist.
- If your login IP address was not blocked for this reason, contact technical support.

**----End**

### Follow-Up Procedure

- **What Should I Do If I Cannot Log In to My Linux ECS?**
- **What Should I Do If I Cannot Log In to My Windows ECS?**

# 3.3 Two-factor Authentication (2FA)

## 3.3.1 How Do I Use 2FA?

This FAQ shows you how to use 2FA.

### Enabling 2FA

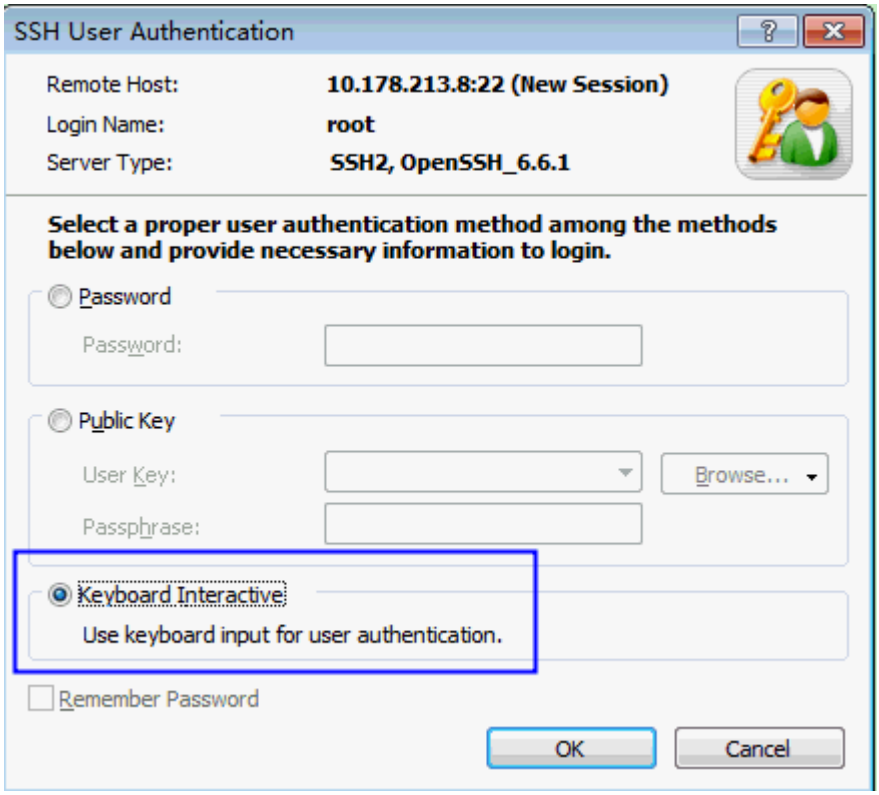
For details, see **Enabling Two-factor Authentication**.


Copyright © Huawei Technologies Co., Ltd.

## 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
       Select **Keyboard Interactive** and click **OK**. See **Figure 3-15**.

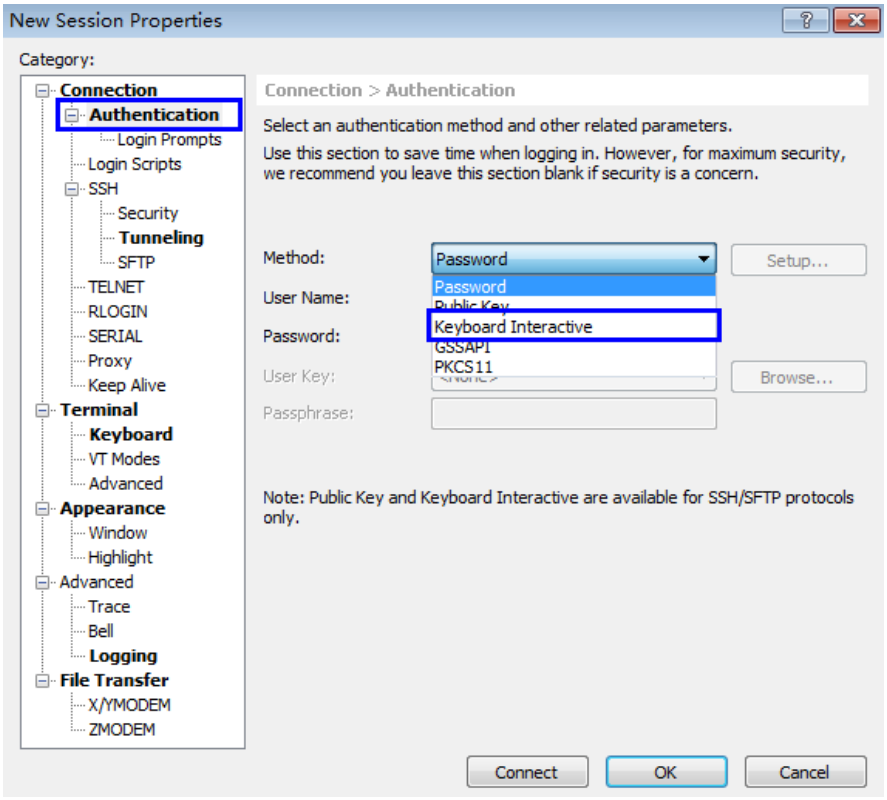
       **Figure 3-15** Keyboard interaction method (1)

     - Xshell
       In the **New Session Properties** dialog box, choose **Connection > Authentication > Method**, choose **Keyboard Interactive** from the **Method** drop-down list, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd. 

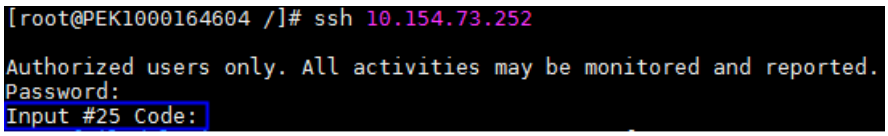
**Figure 3-16** Keyboard interaction method (2)




b. Enter the account and password of the server.

c. Enter the 2FA verification code sent to your terminal, as shown in **Figure 3-17**.

**Figure 3-17** Entering a verification code



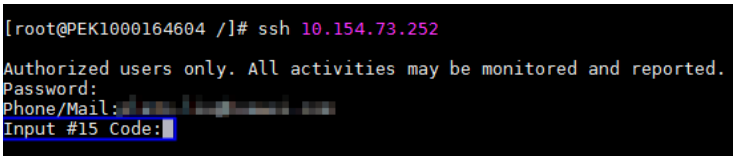


Copyright © Huawei Technologies Co., Ltd.

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 the host 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 3-18**.

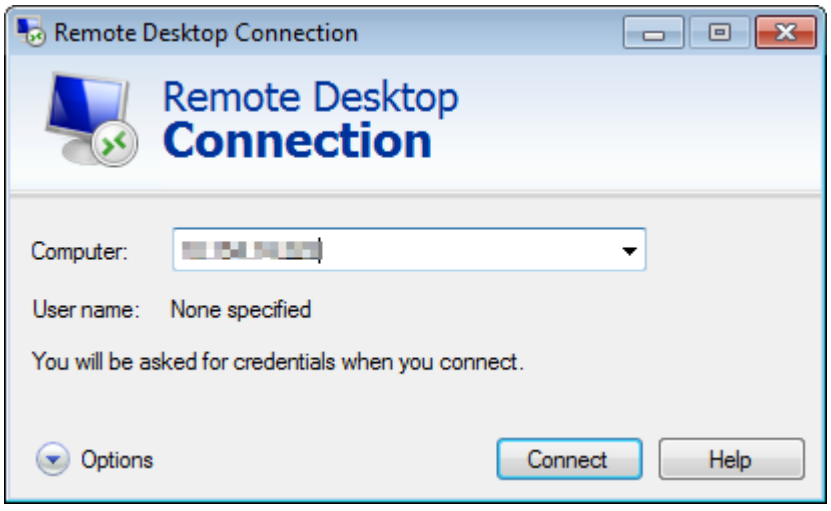
**Figure 3-18** Entering a mobile number or email address




- 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 3-19** 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, host account name, and password on the login page, and click  to log in to the host.


Copyright © Huawei Technologies Co., Ltd.

# 3.3.2 What Do I Do If I Cannot Enable 2FA?

## Symptoms

- There are no servers displayed in the 2FA list.
- 2FA has been enabled but not taken effect.
- 2FA fails to be enabled.

## 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. For details, see "How Do I Change the Login Mode of a Linux ECS from Key Login to Password Login?"
- If it is not, go to **Step 4**.

**Step 4** Check whether you have stopped G01 and 360 Guard (server edition) (if any) on your server.

- If you have, go to **Step 5**.
- If you have not, stop the software.

**Step 5** 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:
    **setenfore 0 #Temporarily disable**
  - To permanently disable the SELinux firewall, run the following command:
    **vi /etc/selinux config**
    **selinux=disabled #Permanently disable**


Copyright © Huawei Technologies Co., Ltd.

**Step 6** Contact technical support.

**----End**

## 3.3.3 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.

  Disable the key pair login mode.

## 3.3.4 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 log in,the following configuration item is required:

PermitRootLogin yes

### Correcting the Login Mode

If you attepted 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: Authenticate your identity and log in again. For details, see **How Do I Use 2FA?**


Copyright © Huawei Technologies Co., Ltd.

NOTE

For details about the prerequisites, restrictions, and limitations for enabling 2FA, see "Enabling 2FA" in **Security Configuration**.

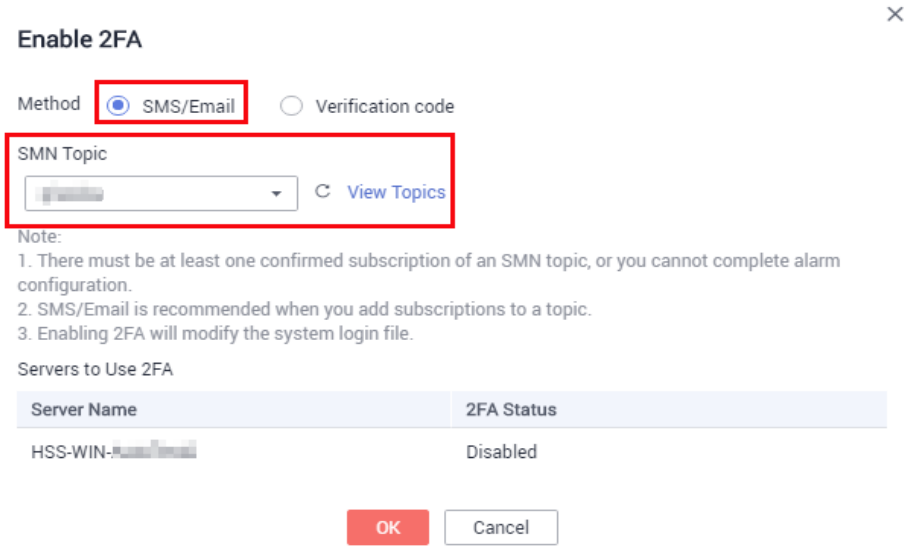
## 3.3.5 How Do I Configure My Mobile Number When Enabling 2FA?

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. For details, see **Creating a Topic**.
- You can use an existing topic (if any), and add or modify mobile phone numbers in the topic as needed. For details, see **Adding a Subscription**.

**Figure 3-20** Setting Method to SMS/Email

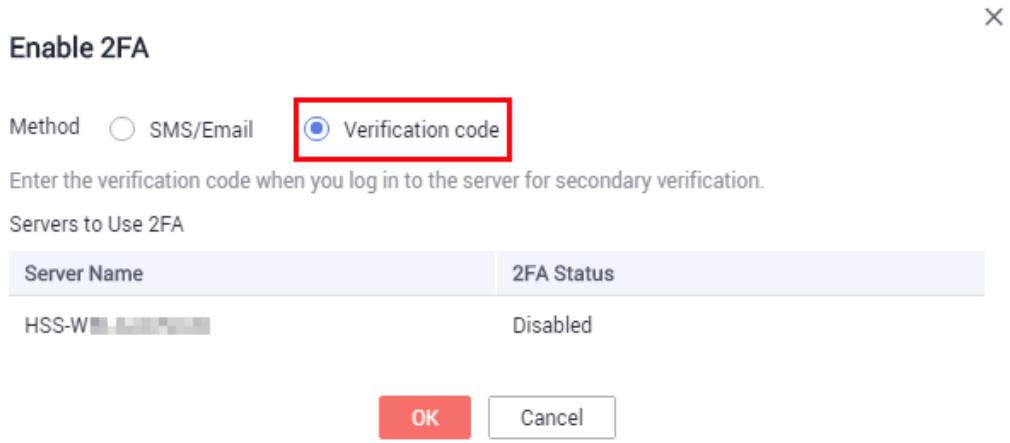



## 3.3.6 If I Choose to Use Verification Code for 2FA, How Do I Get the Code?

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.


Copyright © Huawei Technologies Co., Ltd.

**Figure 3-21** Setting Method to Verification code




# 3.4 HSS Quota

## 3.4.1 How Do I Check My Quotas?

You can check, renew, and unsubscribe from your quota in the server list.

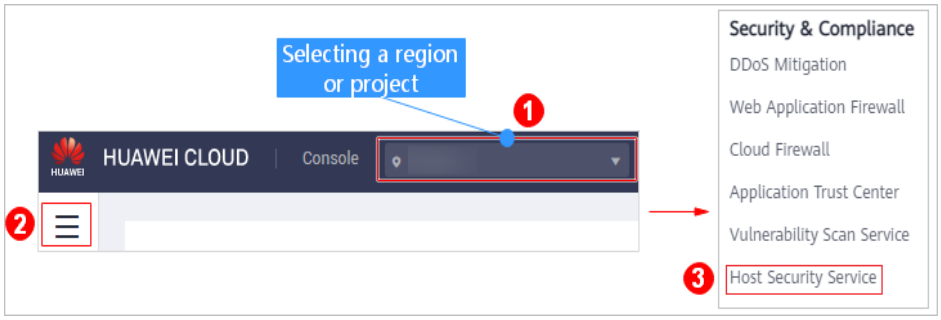
Only the quota purchased in the selected region is displayed. If your quota is not found, ensure you have switched to the correct region and search again.

### Viewing Enterprise/Premium Quota

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

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

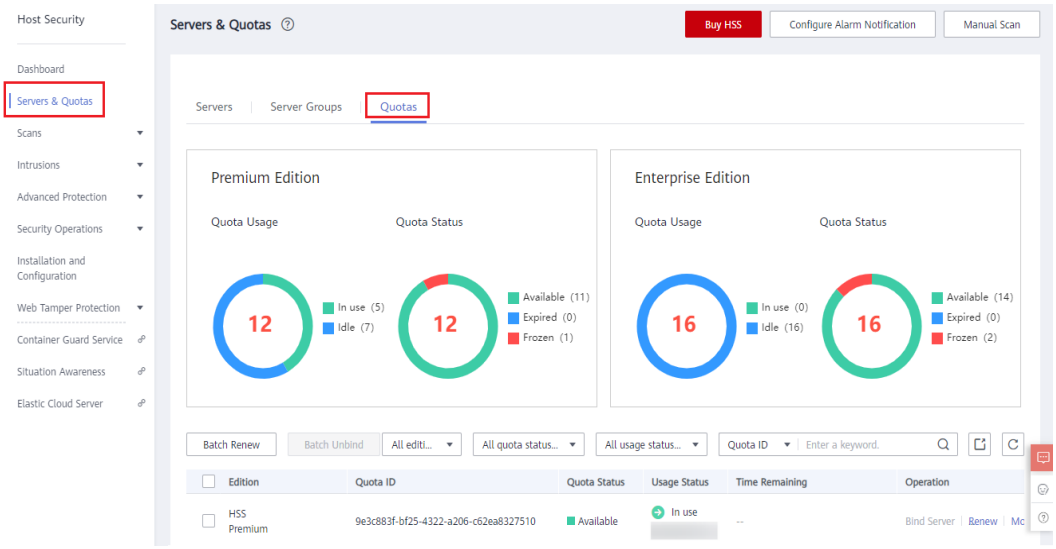
**Figure 3-22** Accessing HSS




**Step 3** On the **Servers & Quotas** page, click the **Quotas** tab.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-23** Viewing the HSS quota




**Step 4** Check quotas and the servers bound to them.

**Table 3-3** Parameters

| Parameter | Description |
| --- | --- |
| Edition | Quota edition |
| Quota ID | Quota ID |
| Quota Status | • **Available**: The quota has not expired and can be used properly.<br>• **Expired**: The quota has expired. During this period, you can still use the quota.<br>• **Frozen**: The quota no longer protects your servers. When the frozen period expires, the quota will be permanently deleted. |
| Usage Status | • **In use**: The quota is being used for a server. The name of the server is displayed below the status.<br>• **Idle**: The quota is not in use. |

 Copyright © Huawei Technologies Co., Ltd. 

**NOTE**

- Binding quota to a server

  Choose **Servers & Quotas**, click the **Quotas** tab, and click **Bind Server** in the **Operation** column.

  A quota can be bound to a server to protect it, on condition that the agent on the server is online.

- Renewal

  You can click **Renew** in the **Operation** column of the quota to renew it. For details, see **How Do I Renew HSS?**

- Unsubscription

  You can click **Unsubscribe** in the **Operation** column of the quota to unsubscribe from it. For details, see **How Do I Unsubscribe from HSS?**

- Unbinding quota

  On the **Quotas** tab of the **Servers & Quotas** page, choose **More** > **Unbind Quota** in the **Operation** column of a quota. HSS will automatically disable protection for the corresponding server and the quota status will change to **Idle**.

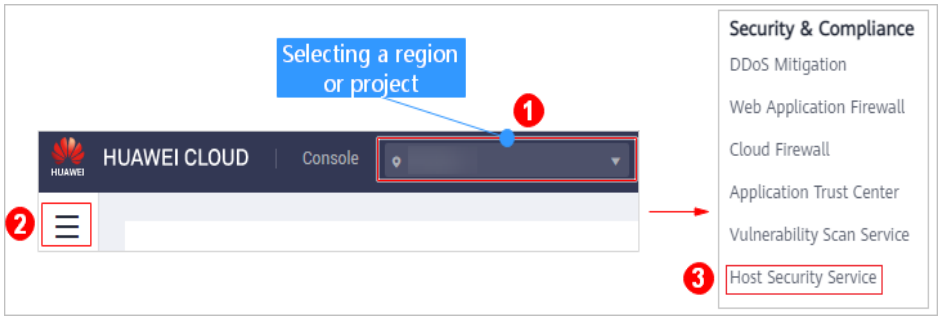
**----End**

## Viewing WTP Quota

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

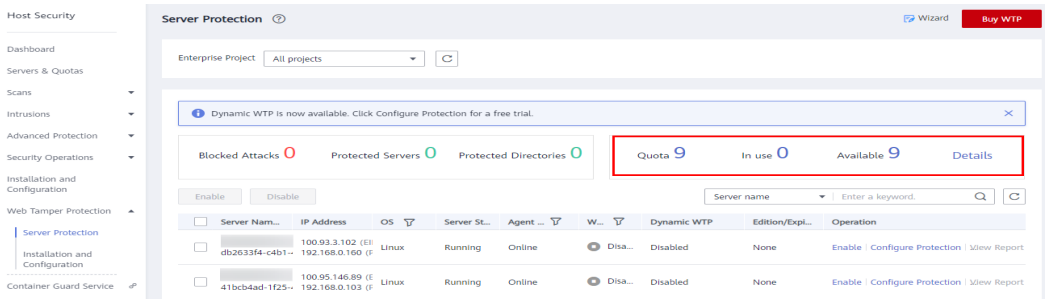
**Step 2** In the upper left corner of the page, select a region, click , and choose **Security & Compliance** > **Host Security Service**.

**Figure 3-24** Accessing HSS




**Step 3** In the navigation pane, choose **Web Tamper Protection**.

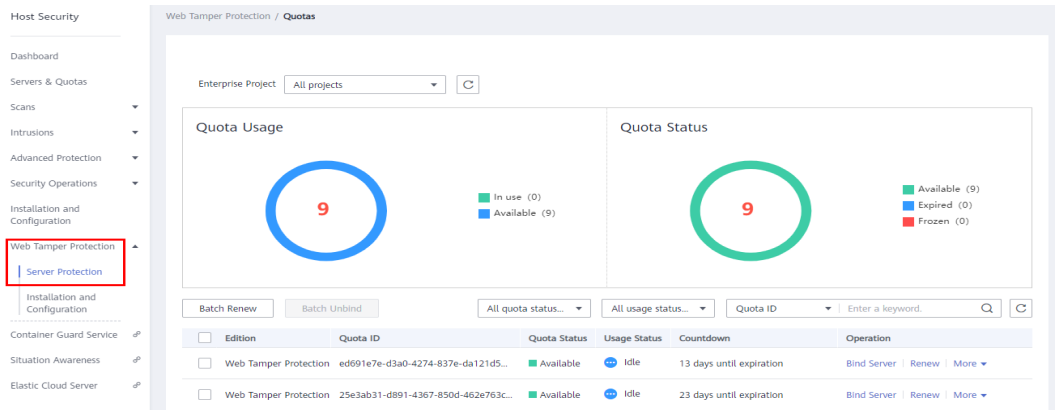
**Figure 3-25** Viewing the WTP edition HSS quota




 Copyright © Huawei Technologies Co., Ltd. 

**Step 4** Click **Details**.

**Figure 3-26** Quota details




**Step 5** Check quota details.

**Table 3-4** Parameters

| Parameter | Description |
| --- | --- |
| Quota Status | • **Available**: The quota has not expired and can be used properly.<br>• **Expired**: The quota has expired. During this period, you can still use the quota.<br>• **Frozen**: The quota no longer protects your servers. When the frozen period expires, the quota will be permanently deleted. |
| Usage Status | • **In use**: The quota is being used for a server. The name of the server is displayed below the status.<br>• **Idle**: The quota is not in use. |

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

- Binding quota to a server

  To enable WTP protection for a server, you can also choose **Web Tamper Protection** > **Server Protection**, click **Details**, and click **Bind Server** in the **Operation** column of a quota.

  A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- Renewal

  You can click **Renew** in the **Operation** column of the edition to renew the subscription to WTP edition HSS. For details, see **How Do I Renew HSS?**
- Unsubscription

  You can click **Unsubscribe** in the **Operation** column of the edition to unsubscribe from the subscription to WTP edition HSS. For details, see **How Do I Unsubscribe from HSS?**
- Unbind Quota

  Choose **Web Tamper Protection** > **Server Protection**, click **Details**, and choose **More** > **Unbind Quota** in the **Operation** column of a quota. HSS will automatically disable WTP for the corresponding server and the quota status will change to **Idle**.

**----End**

## 3.4.2 How Do I Know Whether HSS Has Been Enabled for My Servers?

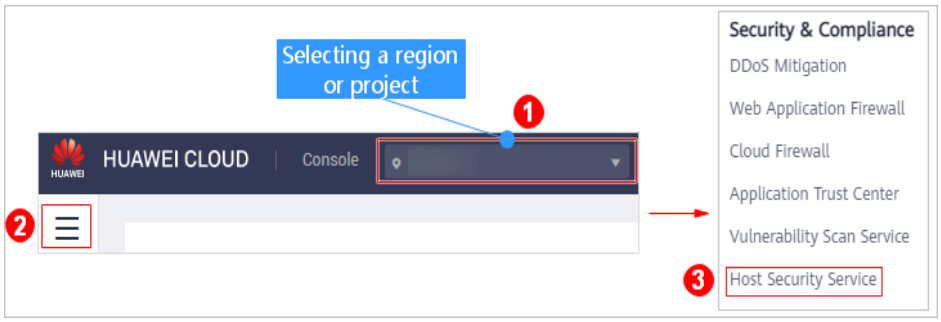
You can check the HSS quota status. For details, see **How Do I Check My Quotas?**

## 3.4.3 How Do I Filter Unprotected Servers?

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

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

**Figure 3-27** Accessing HSS

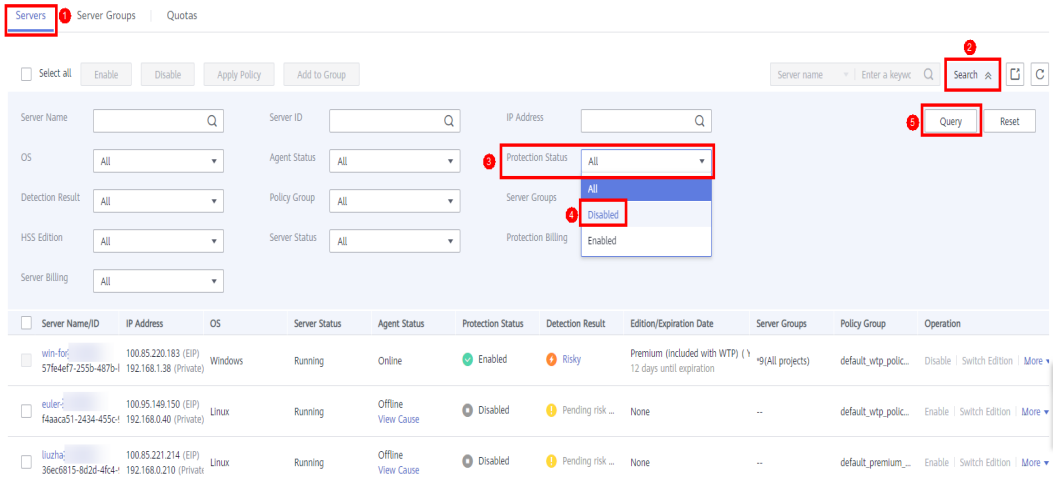



**Step 3** In the navigation pane, choose **Servers & Quotas**.

**Step 4** On the **Servers** tab, filter unprotected servers.

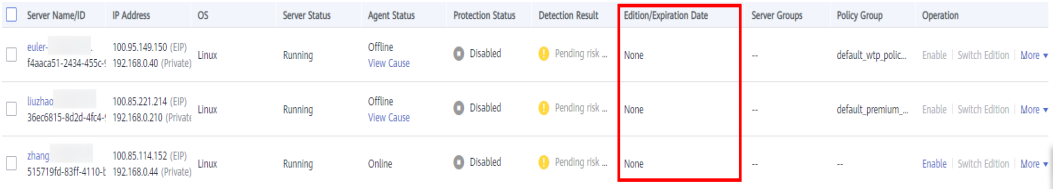
 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-28** Filtering unprotected servers




**Step 5** Check the unprotected servers.

**Figure 3-29** Unprotected servers




**----End**

## 3.4.4 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:

- HUAWEI CLOUD servers purchased in the selected region
- Non-HUAWEI 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.

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

### Checking Your Quota

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

 Copyright © Huawei Technologies Co., Ltd. 

### Checking Your Region

Your quota is available only in the region where you purchased it. If you have purchased quotas but cannot find any on the console, switch to the correct region before enabling protection.

### Checking Your Page

- To enable the basic, enterprise, or premium edition HSS, choose **Host Security Service** > **Servers & Quotas**, and enable it on the **Servers** tab.
- To enable the WTP edition, choose **Web Tamper Protection** > **Server Protection** and then enable it.

### 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.

## 3.4.6 How Do I Allocate a My Quota?

The quotas can be allocated in the following ways:

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

NOTE

Generally, you can let HSS randomly select a quota.

## 3.4.7 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 OSs, such as CentOS and EulerOS; and Windows OSs, such as Windows Server 2012 and 2016.

- Table 3-5 and Table 3-6 list Linux OS versions supported by HSS.

**Table 3-5** Linux OS version (x86 computing)

| No. | OS Version |
| --- | --- |
| 1 | CentOS: 6, 7, and 8 (64 bit) |
| 2 | Debian: 7, 8, 9, and 10 (32/64 bit) |


Copyright © Huawei Technologies Co., Ltd.

| No. | OS Version |
| --- | --- |
| 3 | EulerOS: 2.2, 2.3, and 2.5 (64 bit) |
| 4 | Fedora: 24, 25, and 30 (64 bit) |
| 5 | OpenSUSE: 13.2, 15.0, and 42.2 (64 bit) |
| 6 | Ubuntu: 14.04, 16.04, 18.04, and 20.04 (32/64 bit) |
| 7 | Gentoo: 13.0 and 17.0 (64 bit) |
| 8 | Oracle Linux: 6.9 and 7.4 (64 bit) |

**Table 3-6** Linux OS version (Kunpeng computing)

| No. | OS Version |
| --- | --- |
| 1 | CentOS: 7.4, 7.5, 7.6, and 8.0 64-bit with ARM (40 GB) |
| 2 | EulerOS: 2.8 64-bit with ARM (40 GB) |
| 3 | Fedora: 29 64-bit with ARM (40 GB) |
| 4 | OpenSUSE: 15.0 64-bit with ARM (40 GB) |
| 5 | Ubuntu: 18.04 64-bit with ARM (40 GB) |

- Table 3-7 lists Windows OS versions supported by HSS.

**Table 3-7** Supported Windows OSs

| No. | OS Version | Constraint |
| --- | --- | --- |
| 1 | Windows Server 2019 Datacenter 64-bit English (40 GB) | If a piece of third-party security software, such as McAfee, has been installed on your server, stop the protection function on the software before installing an HSS agent. After you install the agent, you can re-enable the protection function on the software. |
| 2 | Windows Server 2019 Datacenter 64-bit Chinese (40 GB) | |
| 3 | Windows Server 2016 Standard 64-bit English (40 GB) | |
| 4 | Windows Server 2016 Standard 64-bit Chinese (40 GB) | |
| 5 | Windows Server 2016 Datacenter 64-bit English (40 GB) | |
| 6 | Windows Server 2016 Datacenter 64-bit Chinese (40 GB) | |
| 7 | Windows Server 2012 R2 Standard 64-bit English (40 GB) | |

 Copyright © Huawei Technologies Co., Ltd. 

| No. | OS Version | Constraint |
| --- | --- | --- |
| 8 | Windows Server 2012 R2 Standard 64-bit Chinese (40 GB) | |
| 9 | Windows Server 2012 R2 Datacenter 64-bit English (40 GB) | |
| 10 | Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB) | |

# 3.5 Alarm Notifications

## 3.5.1 Will I Be Billed for Alarm Notifications and SMS?

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

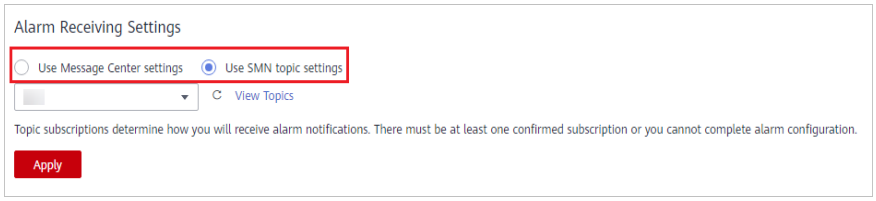
## 3.5.2 How Do I Modify Alarm Notification Recipients?

Recipients can receive alarm notifications via SMS or email.

You can configure recipient information in:

- **Message Center Settings**
- **SMN Topic Settings**

**Figure 3-30** Alarm receiving settings




### Message Center Settings

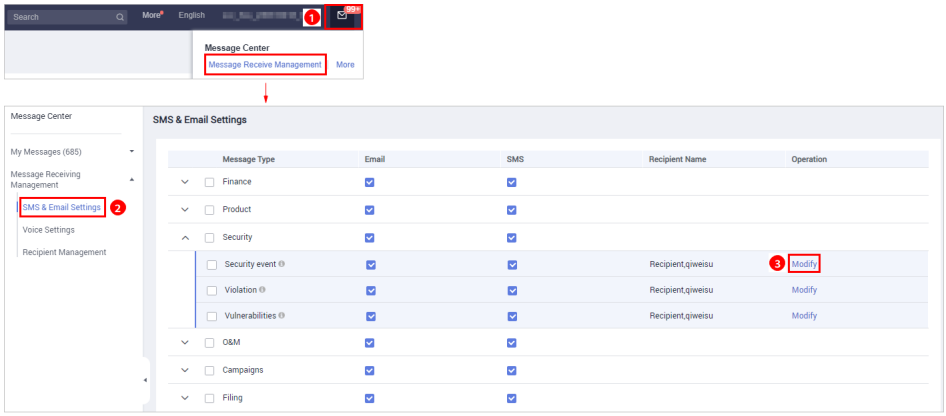
**Step 1** **Log in to the management console.**

**Step 2** Go to the Message Center. Add or change the recipient email address and mobile number in the Message Center.

Go to the Message Center and choose **Message Receiving Management** > **SMS & Email Settings**. In the **Security** area, click **Modify** in the row where **Security event** resides. For details, see **Modifying Recipients of a Message Type**.


Copyright © Huawei Technologies Co., Ltd.

**Figure 3-31** Adding or modifying an alarm notification recipient




**Step 3** In the **Modify Recipient** dialog box, select or deselect the contacts, and click **OK**.

**----End**

## SMN Topic Settings

To change a subscription endpoint (an email address or mobile phone number), delete it and add a new one.

The following procedure changes **test@example.com** to another address in the **HSS-warning** topic.

**Prerequisite**

You have obtained the SMN administrator permission.

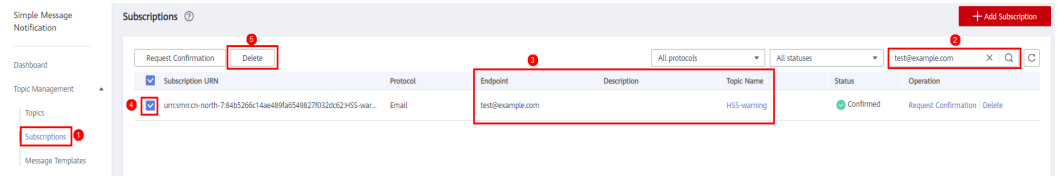
**Procedure**

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

**Step 2** In the upper left corner, click ☰ and choose **Application** > **Simple Message Notification**.

**Step 3** Choose **Topic Management** > **Subscriptions** in the navigation pane. Enter the subscription endpoint in the search box.

**Figure 3-32** Searching for the old subscription endpoint




**Step 4** Confirm that the subscription endpoint receives HSS alarm notifications sent from SMN.

**Step 5** Click **Delete**.

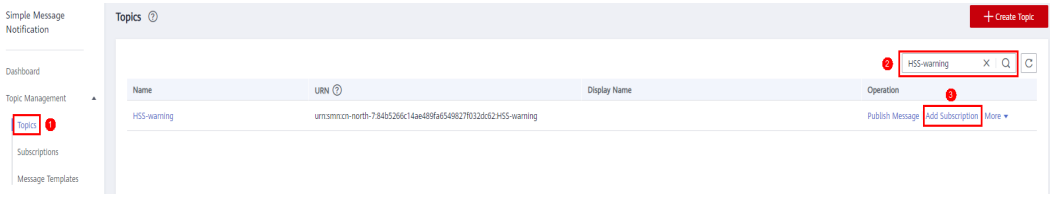
**NOTE**

After a subscription is deleted, the endpoint no longer receives HSS alarm notifications. Exercise caution when performing this operation.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 6** Choose **Topics**, search for the required topic, and add a subscription for it. For details, see **Adding a Subscription** and **Requesting Subscription Confirmation**.

**Figure 3-33** Adding a subscription



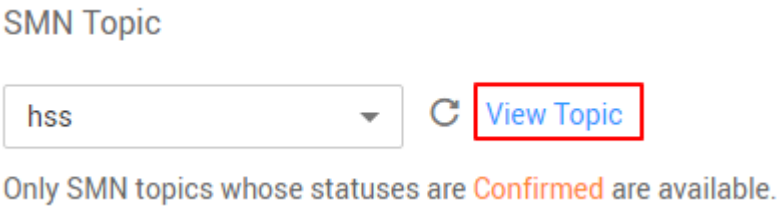

**----End**

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

### No Topics Created

On the **Alarm Notification** page, click **View Topics** in the **SMN Topic** area, and create a topic on the SMN console. For details, see **Creating a Topic**.

**Figure 3-34** 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. For details, see **Adding a Subscription**.

## 3.5.4 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.

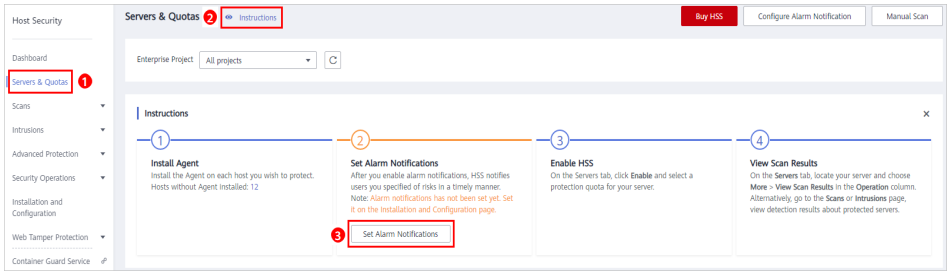
### Setting Alarm Notifications

After you enable HSS, you can use either of the following methods to set alarm notifications:

- Enabling Alarm Notifications for Basic, Professional, or Premium Edition
  - On the **Servers & Quotas** page, click **Set Alarm Notifications** in the **Instructions** area.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-35** Set Alarm Notifications




  - Choose **Installation and Configuration** > **Alarm Notifications**.
- Enabling Alarm Notifications for the WTP Edition

  Choose **Web Tamper Protection** > **Installation and Configuration** > **Alarm Notification**.

## 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 the subscription from the SMN topic.

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

# 3.5.5 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.

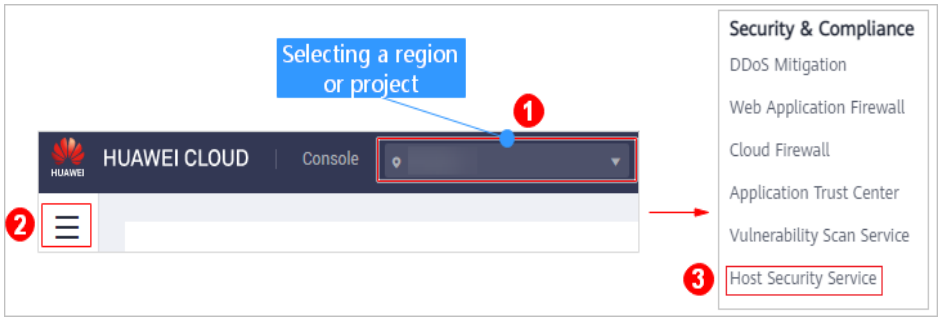
## Enabling Alarm Notifications for Basic, Professional, or Premium Edition

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

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

 Copyright © Huawei Technologies Co., Ltd. 

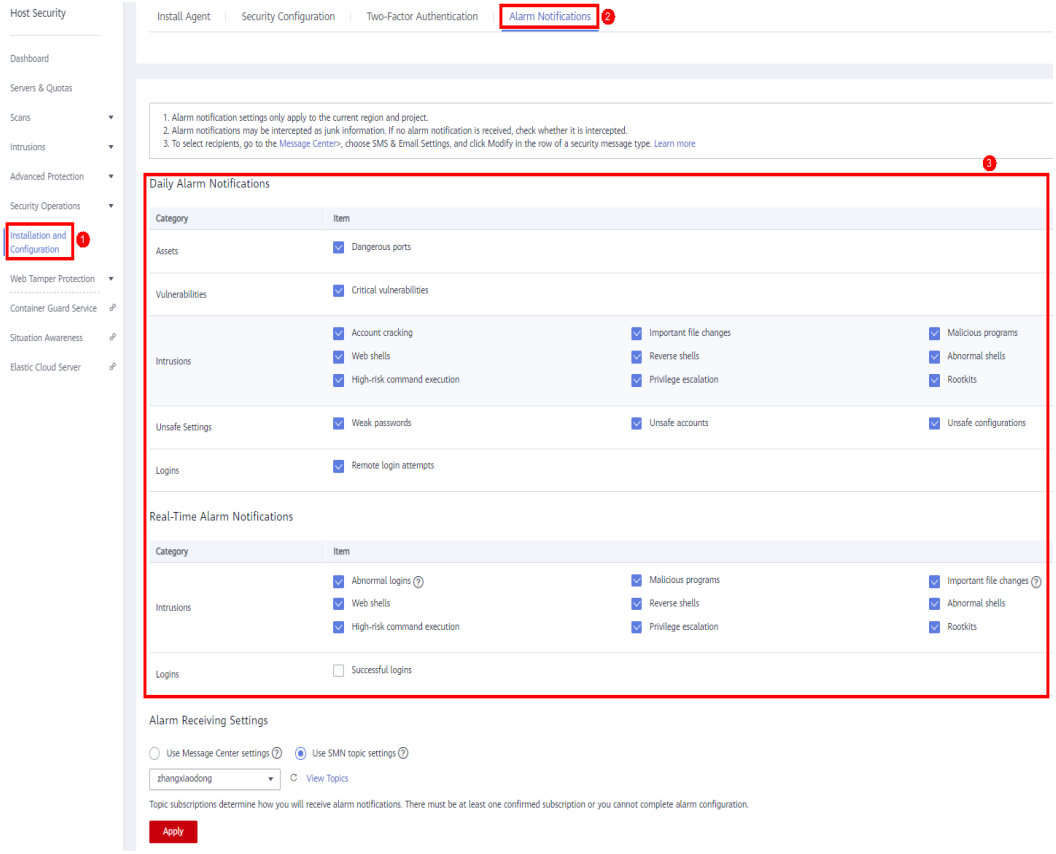
**Figure 3-36** Accessing HSS




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

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

**Figure 3-37** Enabling Alarm Notifications for Basic, Professional, or Premium Edition




**Step 5** Select the notification items for **Daily Alarm Notifications** and **Real-Time Alarm Notifications** as desired. For more information, see **Enabling Alarm Notification**.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 3-8** Notification types

| Type | Description | Suggestion |
| --- | --- | --- |
| Daily alarm notification | The HSS system scans the accounts, web directories, vulnerabilities, malicious programs, and key configurations in the server system at 00:00 every day, and sends the summarized detection results to the recipients you set in the Message Center or SMN, whichever you enabled. | • It is recommended that you receive and periodically check all the content in the daily alarm notification to eliminate risks in a timely manner.<br>• Daily alarm notifications contain a lot of check items. If you want to send the notifications to recipients set in an SMN topic, you are advised to set the topic protocol to **Email**. |
| Real-time alarm notification | When an attacker intrudes a server, HSS sends alarms to the recipients you set in the Message Center or SMN, depending on which one you chose. | • It is recommended that you receive all the content in the real-time alarm notification and view them in time. The HSS system monitors the security of servers in real time, detects the attacker's intrusion, and sends real-time alarm notifications for you to quickly handle the problem.<br>• Real-time alarm notifications are about urgent issues. If you want to send the notifications to recipients set in an SMN topic, you are advised to set the topic protocol to **SMS**. |

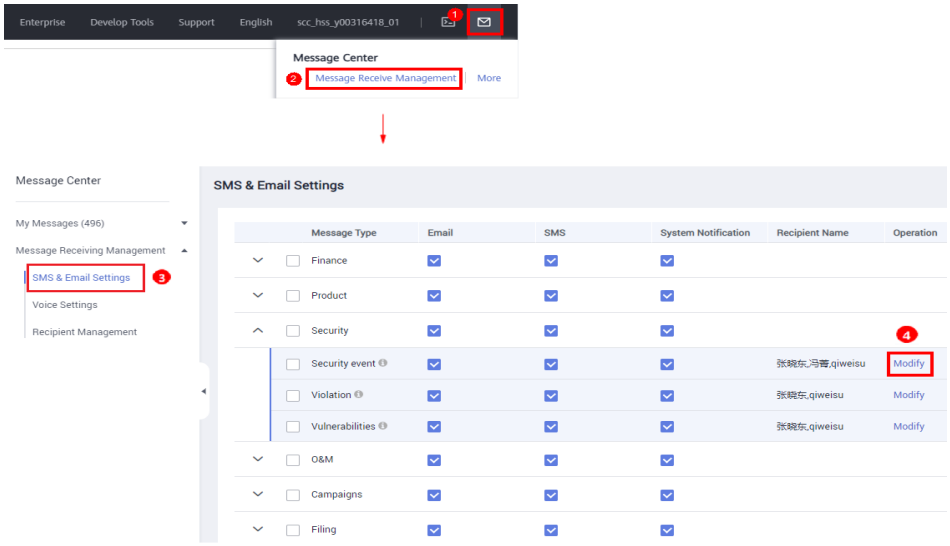
**Step 6** Click **Use Message Center settings** or **Use SMN topic settings**.

- If you click **Use Message Center settings**,

  Go to the Message Center and choose **Message Receiving Management** > **SMS & Email Settings**. In the **Security** area, click **Modify** in the row where **Security event** resides. For details, see **Modifying Recipients of a Message Type**.


Copyright © Huawei Technologies Co., Ltd.

**Figure 3-38** Adding or modifying recipients




- If you click **Use SMN topic settings**, select a topic from the drop-down list.

**Step 7** 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 7**.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

# 4 Alarm and Event Management

## 4.1 How Do I View and Handle Alarms Reported by HSS?

### Viewing Alarms

You can **view details** about alarms on the HSS console.

### Handling Alarms

Fix vulnerabilities, locate and handle intrusions, and modify unsafe settings based on suggestions provided on the HSS console. For details, see **Managing Host Security**.

### Handling Suggestion

- Handle a vulnerability alarm based on suggestions provided on the HSS console. For more information, see **Fixing Vulnerabilities and Verifying the Result**.
- For details about how to handle an intrusion detection alarm, see **Checking and Handling Intrusion Events**.
- For details about how to handle a baseline alarm, see **Suggestions on Fixing Unsafe Settings**.

## 4.2 Brute-force Attack Defense

### 4.2.1 How Does HSS Block Brute-Force Attacks?

#### Protection Scope

HSS can block attacks on MySQL, MS SQL, VSFTP, FileZilla, Serv-U, SSH, and RDP.

If MySQL or VSFTP is installed on your server, after HSS is enabled, the agent will add rules to iptables to prevent MySQL and VSFTP brute force attacks. When

 Copyright © Huawei Technologies Co., Ltd. 

detecting a brute-force attack, HSS will add the source IP address to the blocking list. The added rules are highlighted below.

**Figure 4-1** Added rules

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
IN_HIDS_MYSQLD_BIP_DROP  tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:3306
IN_HIDS_MYSQLD_DENY_DROP  tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:3306

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain IN_HIDS_MYSQLD_BIP_DROP (1 references)
target     prot opt source               destination

Chain IN_HIDS_MYSQLD_DENY_DROP (1 references)
target     prot opt source               destination
```

**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 or VSFTP from brute-force attacks.

## How Brute-Force Attacks Are Blocked

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 for suspicious SSH attacks is 12 hours and that for other suspicious attacks is 24 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 blocking account attacks.

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) or CentOS 8.0 or later, 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.


Copyright © Huawei Technologies Co., Ltd.

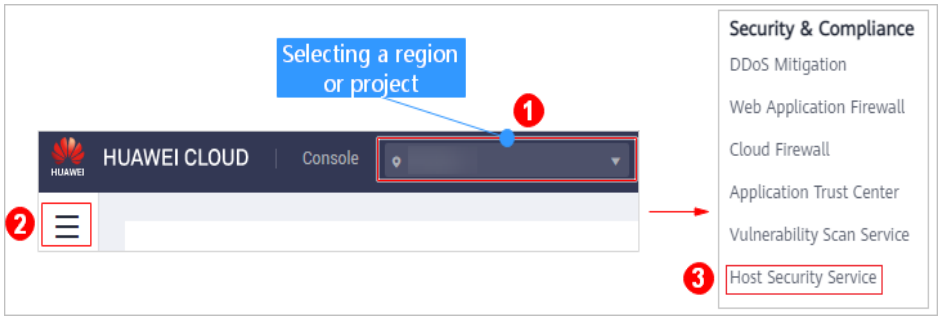
HSS will summarize all attacks in a day in its daily alarm report. You can also view block attacks on the **Intrusions** page of the HSS console.

## Viewing Account Cracking Detection Results

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

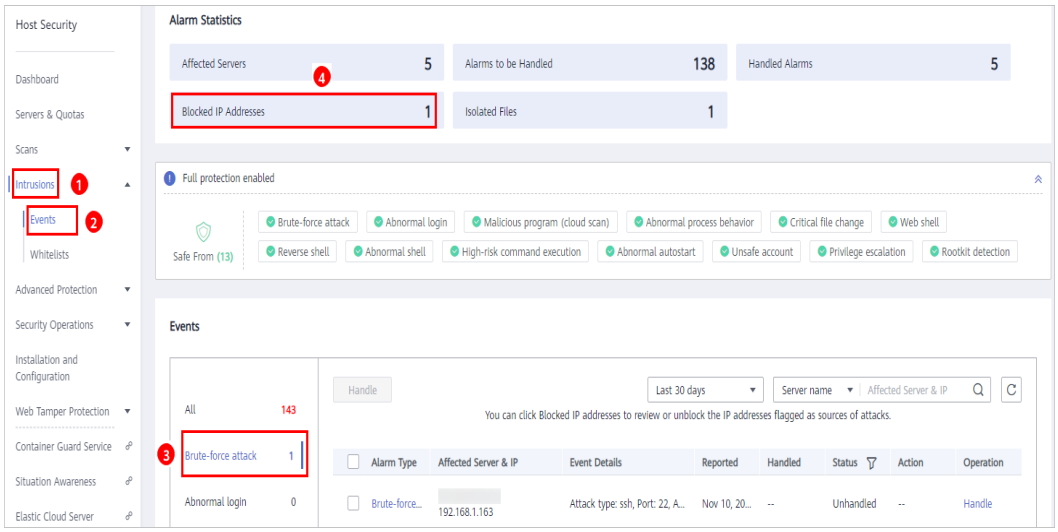
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

**Figure 4-2** Accessing HSS




**Step 3** In the table displayed after you click **Brute-force attack**, you can view blocked attacks on protected servers.

**Figure 4-3** Brute-force attack




**Step 4** Click **Blocked IP Addresses** to check the source IP addresses, attack types, number of intercepted attacks, the time of the first and last interceptions, and the interception status.

- **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.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.

**----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 reach the threshold again, this IP address will be blocked again.

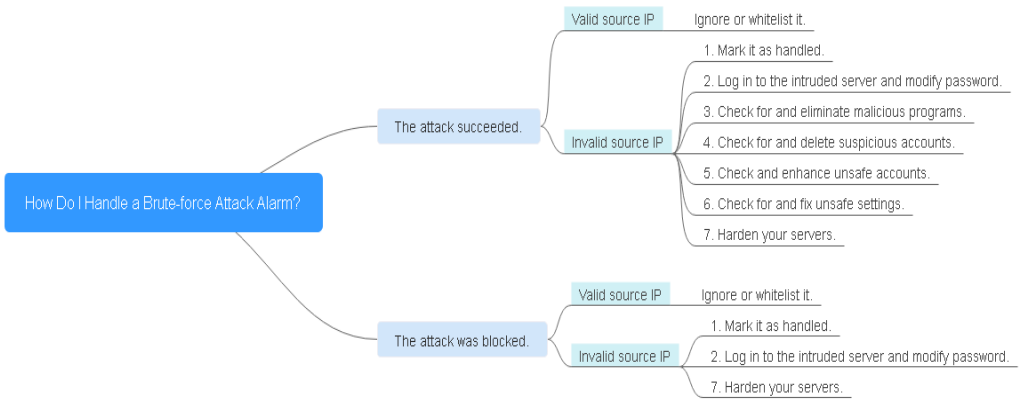
## 4.2.2 How Do I Handle a Brute-force Attack Alarm?

- 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 4-4** Troubleshooting




 Copyright © Huawei Technologies Co., Ltd. 

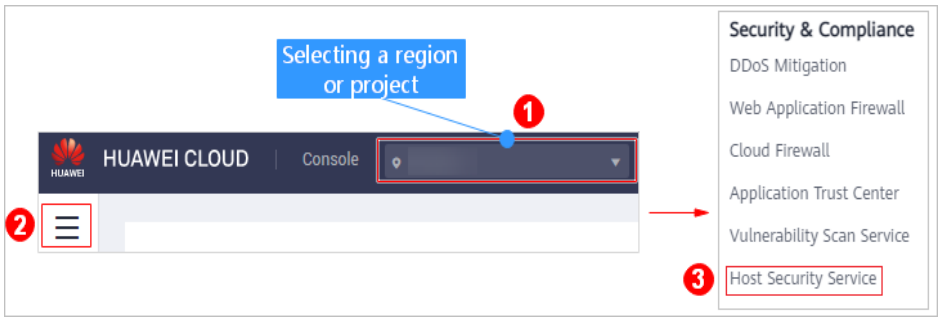
## Handling the Alarm of a Successful Brute-force Attack

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** > **Host Security Service**.

**Figure 4-5** Accessing HSS



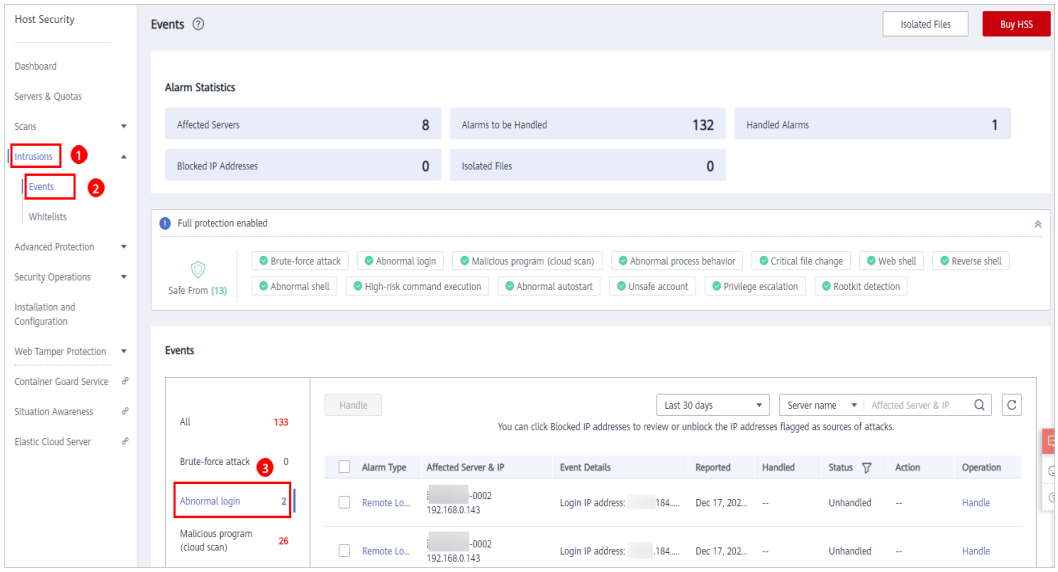

**Step 3** Check whether the IP address that triggered the alarm is valid.

Choose **Intrusions** > **Events**. In the **Events** area, click **Abnormal login** and 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 4-6** Abnormal logins




 Copyright © Huawei Technologies Co., Ltd. 

**Step 4** Check for and eliminate malicious programs.

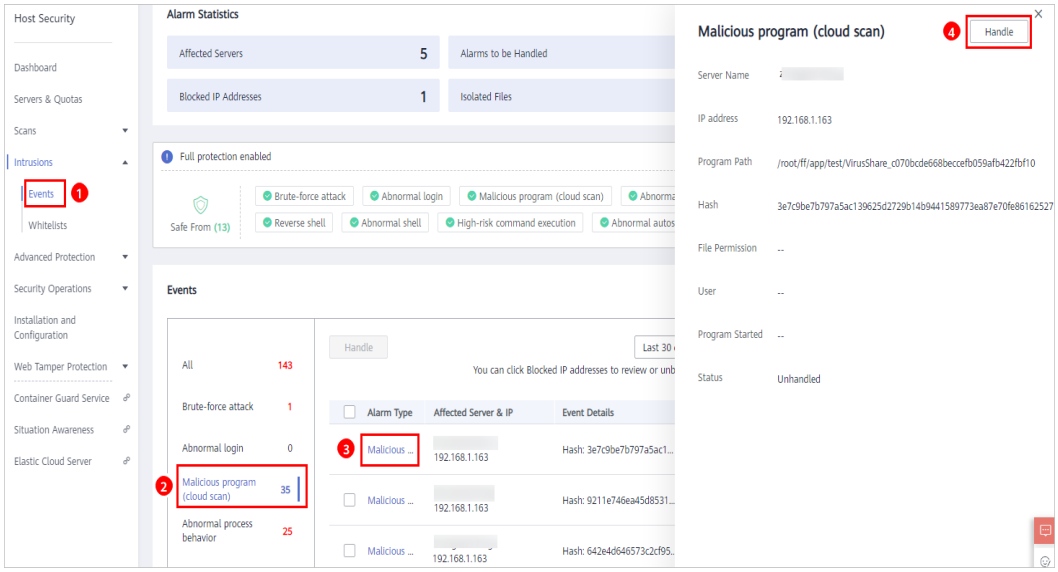
Click **Malicious program (cloud scan)** and check alarm events.

- 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 row of this event and select **Isolate and kill**.

- If you have confirmed that all the malicious program alarms are false, go to **Step 5**.

**Figure 4-7** Malicious program (cloud scan)




**Step 5** Check for and delete suspicious accounts.

Choose **Scans** > **Assets** and click the **Account Information** tab. Delete suspicious accounts to prevent attackers from creating accounts or escalating account permissions (for example, adding login permissions to an account). For details, see **Managing Account Information**.

**Step 6** Check and enhance unsafe accounts.

Choose **Intrusions** > **Events**. In the **Events** area, click **Unsafe account**. For details, see **Handling Suggestion**.

**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 **Suggestions on Fixing Unsafe Settings**.

**Step 8** Harden your servers.

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

 Copyright © Huawei Technologies Co., Ltd. 

## Handling the Alarm of a Blocked Brute-force Attack

Check whether blocked IP addresses can be trusted. 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.

**Constraints and Limitations**

- Linux OS

  On servers running the EulerOS with ARM, or Centos 8.0 or later, HSS does not block the IP addresses suspected of SSH brute-force attacks, but only generates alarms.

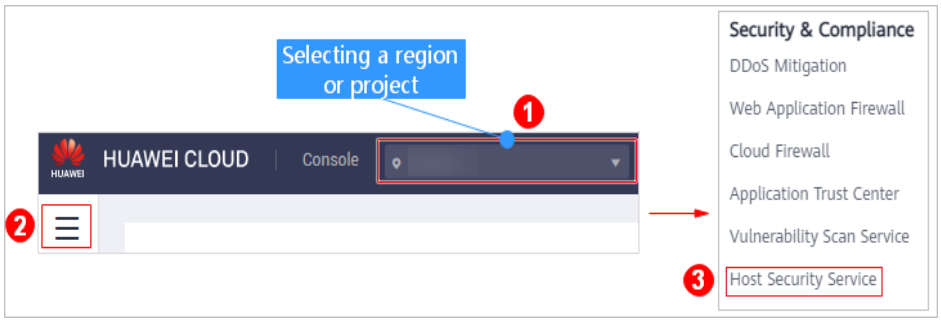
- Windows OS
  - Authorize the Windows firewall when you enable protection for a Windows server. Do not disable the Windows firewall during the HSS in-service period. If the Windows firewall is disabled, HSS cannot block brute-force attack IP addresses.
  - If the Windows firewall is manually enabled, HSS may also fail to block brute-force attack IP addresses.

**Procedure**

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

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

**Figure 4-8** Accessing HSS



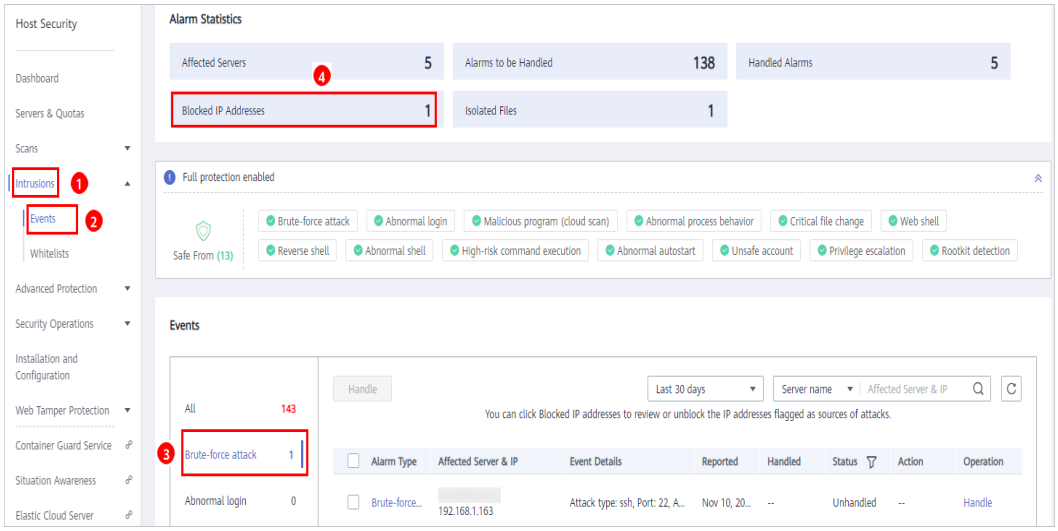

**Step 3** Choose **Intrusions** > **Events**. In the **Events** area, click **Brute-force attack**.

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.


Copyright © Huawei Technologies Co., Ltd.

**Figure 4-9** Brute-force attacks




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

- If the IP address is valid,
  - To handle a false alarm, click **Handle** in the row of the alarm event. Ignore or whitelist the IP address.

    This does not unblock the IP address.
  - To unblock the IP address, click **Blocked IP Address** in the **Alarm Statistics** area, select the IP address, and unblock it. Alternatively, you can just wait for it to be automatically unblocked when its blocking duration expires.

    By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours.
- If the source IP address is invalid or unknown,

  Mark this event 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 Block Brute-Force Attacks?**
- **How Do I Unblock an IP Address?**

# 4.2.3 How Do I Defend Against Brute-force Attacks?

## Attack Sources

An attack can come from inside or outside HUAWEI CLOUD.

For details about how to handle and prevent attacks from inside HUAWEI CLOUD, see **How Do I Handle Alarms on the Brute-Force Attacks Launched from a HUAWEI CLOUD IP Address?** and **Preventive Measures**.

 Copyright © Huawei Technologies Co., Ltd. 

For details about how to handle and prevent attacks from outside HUAWEI CLOUD, see **How Do I Handle a Brute-force Attack Alarm?** and **Preventive Measures**.

## Preventive Measures

Configure your security products, applications, and networks to enhance security.

- **Configuring security products**
  - **CBH**

    CBH can help you manage server resources and application servers in a unified manner. It provides login authentication, resource management, and session audit functions. For more information about CBH, see **Features** and **Getting Started**.

    Intrusions and crackings will first be monitored and blocked by CBH and then by HSS.
- **Applications**
  - **Using SSH keys for login**

    Enable SSH key login for server resources and application servers. A user can log in only if its private key matches the public key. For details about how to create a key pair, see **Creating a Key Pair**.
  - **Enabling 2FA**

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

    Choose **Installation and Configuration**. On the **Two-Factor Authentication** tab, select servers and click **Enable 2FA**. For details, see **Enabling 2FA**.
- **Network**
  - **Configuring the SSH login whitelist**

    The SSH login whitelist allows logins from only whitelisted IP address to prevent account cracking. For details, see **Configuring an SSH Login IP Address Whitelist**.
  - **Using non-default ports**

    Change the default remote management ports 22 and 3389 to other ports. For details, see **How Can I Change a Remote Login Port?**
  - 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).

    HSS **prevents brute-force attacks** on server accounts in real time and blocks attack source IP addresses. 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.


Copyright © Huawei Technologies Co., Ltd.

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 4-1** Setting IP addresses to remotely connect to ECSs

| Direction | Protocol/ Application | Port | Source IP Address |
| --- | --- | --- | --- |
| 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.

  For details, see **How Do I Install a PAM and Set a Proper Password Complexity Policy?** and **How Do I Set a Secure Password?**

## 4.2.4 What Do I Do If the Account Cracking Prevention Function Does Not Take Effect on Some Accounts for Linux Servers?

### Possible Causes

The dependency, **libwrap.so**, which sshd in the host system depends on, is missing.

NOTE

As a free software library, libwrap implements the universal TCP Wrapper function. Any daemon that contains **libwrap.so** can use the rules in files **/etc/hosts.allow** and **/etc/hosts.deny** to perform simple access control on the host.

### Solution

Log in to the server and install the HSS agent. For details, see **Installing an HSS Agent** (the server must be associated with an EIP). Then run the following command:

**sh /usr/local/hostguard/conf/config_ssh_xinetd.sh**.

### Affected Image Versions

- The following are Gentoo images that have the problem:
  - Gentoo Linux 17.0 64bit (40 GB)
  - Gentoo Linux 13.0 64bit (40 GB)
- The following are OpenSUSE images that have the problem:
  - OpenSUSE 42.2 64bit (40 GB)
  - OpenSUSE 13.2 64bit (40 GB)


Copyright © Huawei Technologies Co., Ltd.

# 4.2.5 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

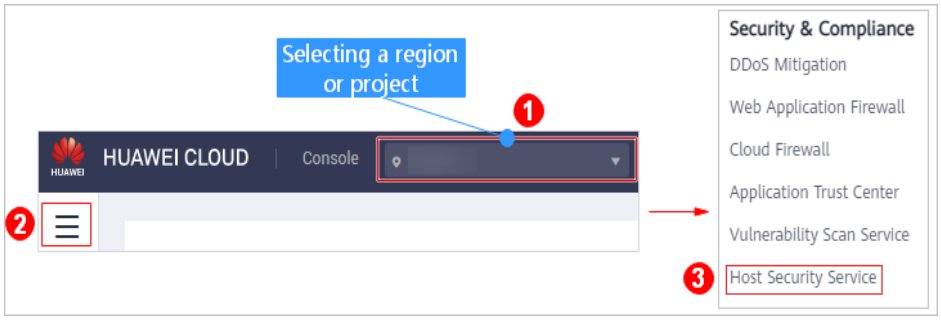
- By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours.
- If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.

## 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** > **Host Security Service**.

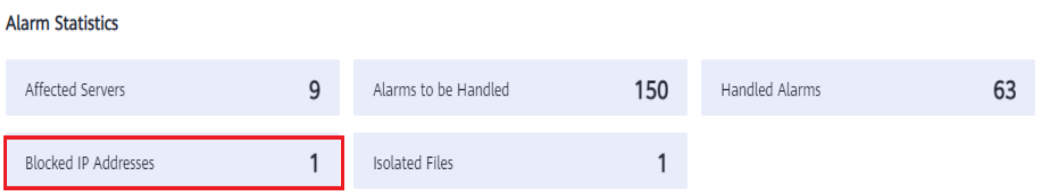
**Figure 4-10** Accessing HSS




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

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

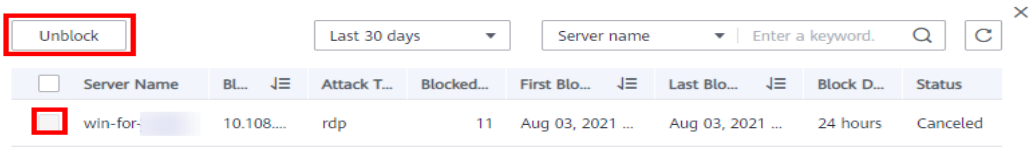
**Figure 4-11** Blocked IP addresses




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


Copyright © Huawei Technologies Co., Ltd.

**Figure 4-12** Unblocking an IP address




**----End**

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

Possible cause: 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.

1. Configure a whitelist.
2. Use another port.
3. Configure security group rules.
4. Enable 2FA.
5. Configure a strong password.

For details, see **How Do I Defend Against Brute-force Attacks?**

## 4.2.7 How Do I Handle Alarms on the Brute-Force Attacks Launched from a HUAWEI CLOUD IP Address?

### Possible Cause

Some HUAWEI CLOUD 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 **Editions**.


Copyright © Huawei Technologies Co., Ltd.

# 4.3 Weak Passwords and Unsafe Accounts

## 4.3.1 How Do I Handle a Weak Password Alarm?

Servers using weak passwords are exposed to intrusions. If a weak password alarm is reported, change the password that triggered the alarm immediately.

### Causes

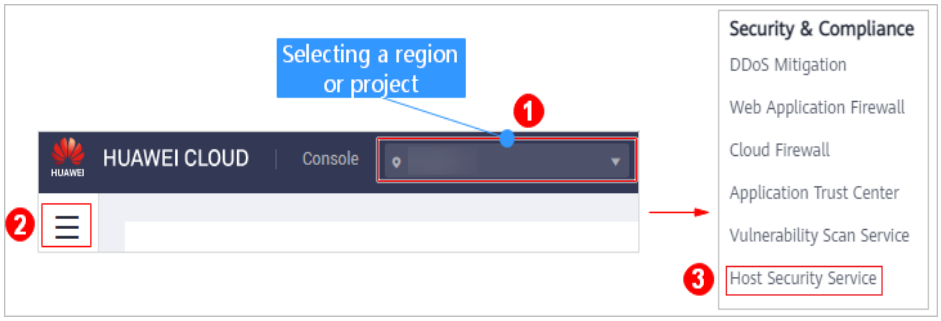
- If simple passwords are used and match those in the weak password library, a weak password alarm will be generated.
- A password used by multiple member accounts will be regarded as a weak password and trigger an alarm.

### 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** > **Host Security Service**.

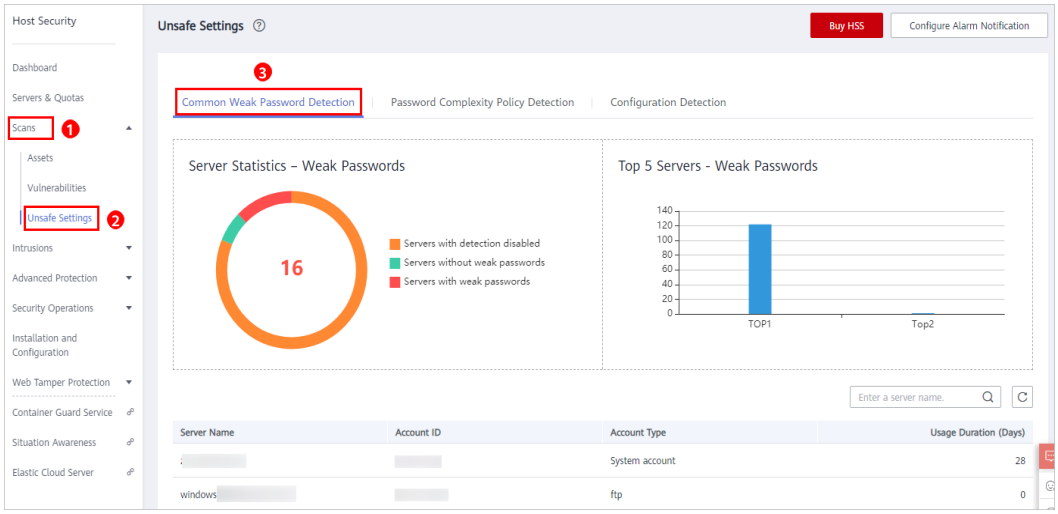
**Figure 4-13** Accessing HSS




**Step 3** Choose **Scans** > **Unsafe Settings** and click the **Common Weak Password Detection** tab.


Copyright © Huawei Technologies Co., Ltd.

**Figure 4-14** 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:<br>1. Log in to the Windows OS.<br>2. Click  in the lower left corner and click .<br>3. In the **Windows Settings** window, click **Accounts**.<br>4. Choose **Sign-in options** from the navigation tree.<br>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:<br>**passswd [*<user>*]** | If you do not specify any username, you are changing the password of the current user.<br>After the command is executed, enter the new password as prompted.<br>**NOTE**<br>Replace *<user>* with the username. |

 Copyright © Huawei Technologies Co., Ltd. 

| System | Procedure | Remarks |
| --- | --- | --- |
| MySQL database | 1. Log in to the MySQL database.<br>2. Run the following command to check the database user password:<br>**SELECT user, host, authentication_string From user;**<br>This command is probably invalid in certain MySQL versions.<br>In this case, run the following command:<br>**SELECT user, host password From user;**<br>3. Run the following command to change the password:<br>**SET PASSWORD FOR'*Username*'@'*Host*'=PASSWORD('*New_password*');**<br>4. Run the following command to refresh password settings:<br>**flush privileges;** | None |
| Redis database | 1. Open the Redis database configuration file **redis.conf**.<br>2. Run the following command to change the password:<br>**requirepass *<password>*;** | • If there is already a password, the command will change it to the new password.<br>• If there has been no password set, the command will set the password.<br>**NOTE**<br>Replace *<password>* with the new password. |
| Tomcat | 1. Open the **conf/tomcat-user.xml** configuration file in the Tomcat root directory.<br>2. Change the value of **password** under the **user** node to a strong password. | None |

## 4.3.2 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:

 Copyright © Huawei Technologies Co., Ltd. 

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: space and `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
c. The password cannot be the username or the username in reverse order.

   Bad password examples: **administrator**, **test**, **root**, **oracle**, **mysql**

- 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

    Bad examples: **123456**, **abcdef**, **123abc**, **qwerty**, **1qaz2wsx**, **!QAZxsw2**, **qazxsw**, **1qaz@WSX**, **1q2w3e**, **123456789**, **password**
  - Phrases

    Bad examples: **143**, **iloveyou**
  - 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.

## 4.3.3 Why Are the Weak Password Alarms Still Reported After the Weak Password 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 enhance the passwords of the accounts used for logging in to servers, such as SSH accounts.

 Copyright © Huawei Technologies Co., Ltd. 

- To protect internal data of your servers, you are advised to enhance the passwords of software accounts, 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.

# 4.4 Intrusions

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

Take immediate measures to contain the attack and kill mining programs, preventing miners from occupying CPU or affecting other applications.

You should also harden your servers to better block intrusions.

### Checking For and Clearing Mining Programs

#### Mind Map for Troubleshooting

The following mind map describes how to identify mining programs and the root cause for their intrusion.

**Figure 4-15** Mind map for troubleshooting



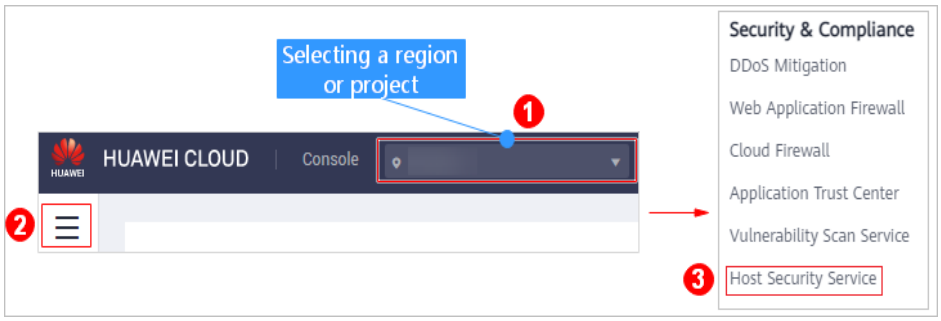

#### Procedure

**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** > **Host Security Service**.

 Copyright © Huawei Technologies Co., Ltd. 

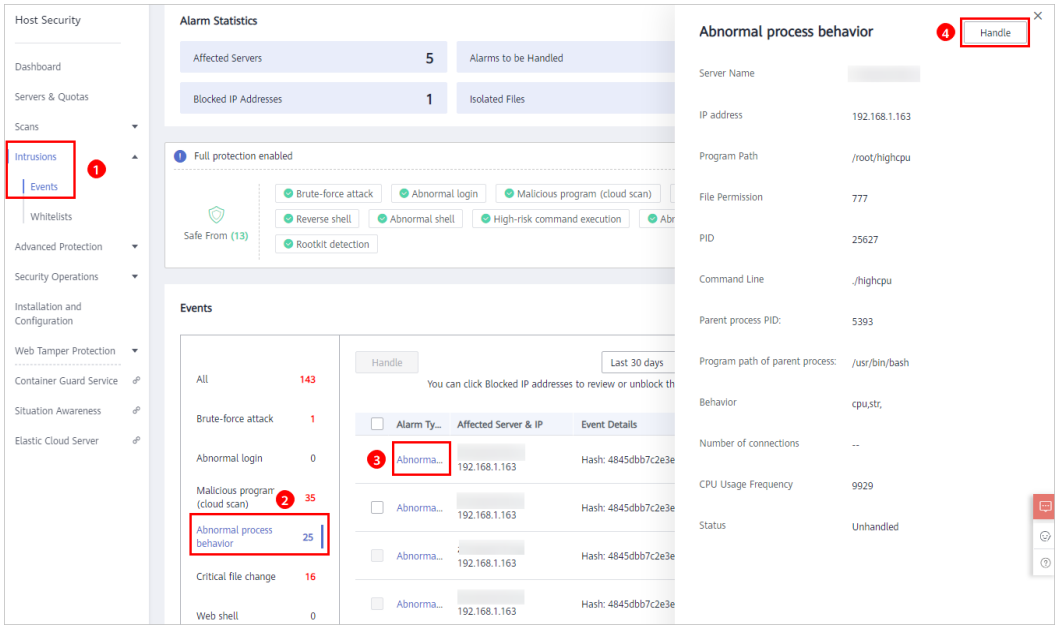
**Figure 4-16** Accessing HSS




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

Choose **Intrusions** > **Events**. In the **Events** area, click **Abnormal process behavior**. Click **Handle** in the **Operation** column of an event.

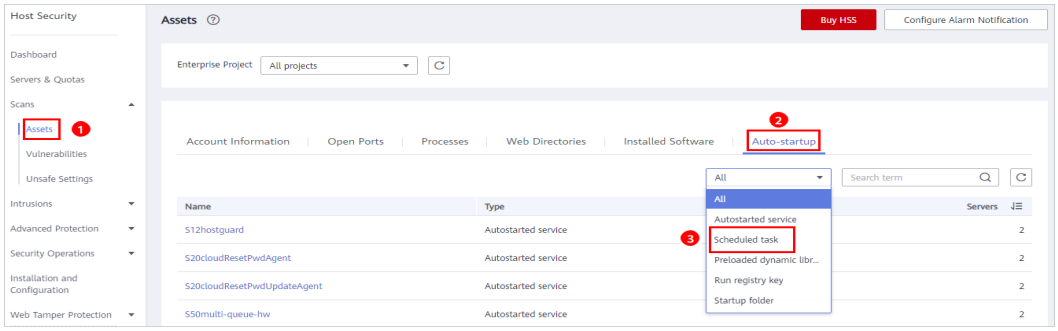
**Figure 4-17** Handling abnormal process behavior




**Step 4** Check scheduled tasks. Some of your scheduled tasks were probably created by attackers to periodically download mining programs or run mining scripts.

Choose **Scans** > **Assets** and click **Auto-startup**. In the drop-down list, select **Scheduled task**, and check for and stop suspicious tasks.

**Figure 4-18** Checking scheduled tasks

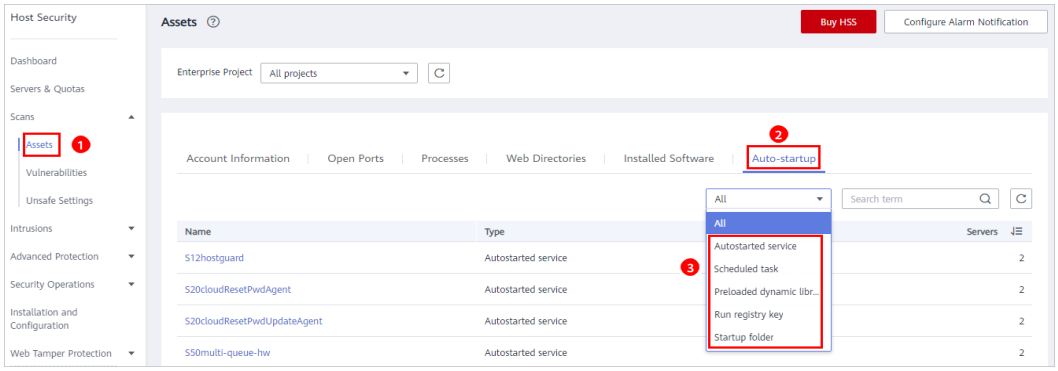



 Copyright © Huawei Technologies Co., Ltd. 

**Step 5** Check auto-startup items. Some of your auto-startup items were probably created by attackers to start mining programs upon server restart.

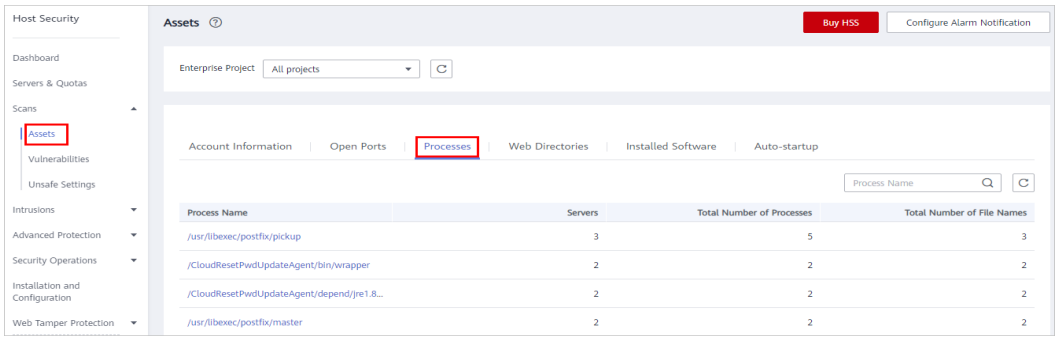
Choose **Scans** > **Assets** and click **Auto-startup**. Filter and check **Autostarted service**, **Preloaded dynamic library**, **Run registry key**, and **Startup folder** items.

**Figure 4-19** Checking auto-startup items



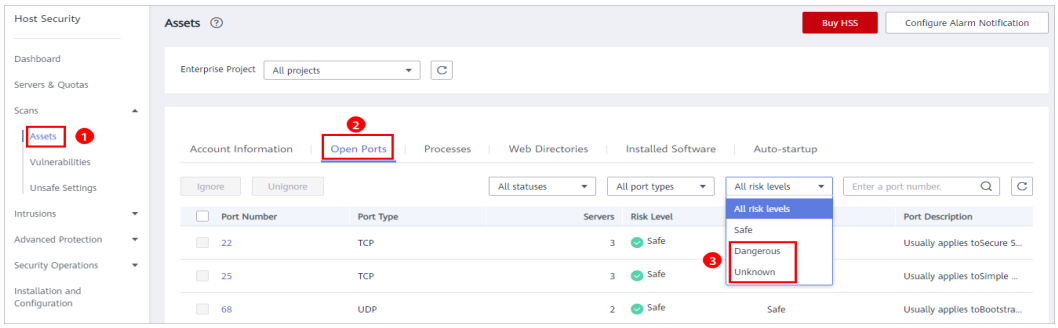

**Step 6** Check for and terminate suspicious processes.

**Figure 4-20** Checking for suspicious processes




**Step 7** Check for and disable dangerous or unknown ports.

**Figure 4-21** Checking open ports




**Step 8** Verify that the mining program has been deleted and cannot be recovered. If it still exists, reinstall your server OS.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 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. For details, see **Quickly Learning Your Host Security Status**.
2. Set stronger passwords for all accounts (including system and application accounts), or change the login mode to key-based login.
   - For details about password settings, see **How Do I Set a Secure Password?**
   - For details about key-based login, 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**.<br>• Disable and delete unnecessary accounts. (You are advised to disable inactive accounts for three months before deleting them.) | 1. Open **Control Panel**.<br>2. Click **Administrative Tools**. Open **Computer Management**.<br>3. Choose **System Tools** > **Local Users and Groups** > **Users**.<br>4. Double-click **Guest**. In the **Guest Properties** window, select **Account is disabled**.<br>5. Click **OK**. |
| Assign accounts with only necessary permissions to users. | Create users and user groups of specific types.<br>Example: administrators, database users, audit users | 1. Open **Control Panel**.<br>2. Click **Administrative Tools**. Open **Computer Management**.<br>3. Choose **System Tools** > **Local Users and Groups**. Create users and groups as needed. |

 Copyright © Huawei Technologies Co., Ltd. 

| Measure | Description | Procedure |
| --- | --- | --- |
| Periodically check and delete unnecessary accounts. | Periodically delete or lock unnecessary accounts. | 1. Open **Control Panel**.<br>2. Click **Administrative Tools**. Open **Computer Management**.<br>3. Choose **System Tools** > **Local Users and Groups**.<br>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**.<br>2. Click **Administrative Tools**. Open **Local Security Policy**.<br>3. Choose **Local Policies** > **Security Options**.<br>4. Double-click **Interactive logon: Do not display last user name**.<br>5. In the **Interactive logon: Do not display last user name Properties** window, click **Enabled** and click **OK**. |

- **Password hardening**

| Setting | Description | Procedure |
| --- | --- | --- |
| Complexity | Passwords must meet the complexity requirements in **How Do I Set a Secure Password?** | 1. Open **Control Panel**.<br>2. Click **Administrative Tools**. Open **Local Security Policy**.<br>3. Choose **Account Policies** > **Password Policy**.<br>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**.<br>2. Click **Administrative Tools**. Open **Local Security Policy**.<br>3. Choose **Account Policies** > **Password Policy**.<br>4. Set **Maximum password age** to 90 days or shorter. |


Copyright © Huawei Technologies Co., Ltd.

| Setting | Description | Procedure |
| --- | --- | --- |
| 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**.<br>2. Click **Administrative Tools**. Open **Local Security Policy**.<br>3. Choose **Account Policies** > **Account Lockout Policy**.<br>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**.<br>2. Click **Administrative Tools**. Open **Local Security Policy**.<br>3. Choose **Local Policies** > **User Rights Assignment**.<br>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**.<br>2. Click **Administrative Tools**. Open **Local Security Policy**.<br>3. Choose **Local Policies** > **User Rights Assignment**.<br>4. Assign the permission **Shut down the system** only to the **Administrators** group. |
| User rights assignment | Assign the permission **Take ownership of files or other objects** only to the **Administrators** group. | 1. Open **Control Panel**.<br>2. Click **Administrative Tools**. Open **Local Security Policy**.<br>3. Choose **Local Policies** > **User Rights Assignment**.<br>4. Assign the permission **Shut down the system** only to the **Administrators** group. |


Copyright © Huawei Technologies Co., Ltd.

| Authorization | Description | Procedure |
| --- | --- | --- |
| Login | Authorize users to log in to the computer locally. | 1. Open **Control Panel**.<br>2. Click **Administrative Tools**. Open **Local Security Policy**.<br>3. Choose **Local Policies** > **User Rights Assignment**.<br>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). | 1. Open **Control Panel**.<br>2. Click **Administrative Tools**. Open **Local Security Policy**.<br>3. Choose **Local Policies** > **User Rights Assignment**.<br>4. Assign the permission **Access this computer from the network** to the users you want to authorize. |

## 4.4.2 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.

### Isolating and Killing a Malicious Program

- Choose **Installation and Configuration** and click the **Security Configuration** tab. Click the **Isolation and Killing of Malicious Programs** tab and enable this function.
- Choose **Intrusions** > **Events**. 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

- Choose **Intrusions** > **Events**. Click **Isolated Files** in the upper right corner. Cancel the isolation of the whitelisted file.
- Choose **Intrusions** > **Events**. In the **Events** area, manually cancel the isolation and killing of the whitelisted file.

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


Copyright © Huawei Technologies Co., Ltd.

## 4.4.3 What Should I Do If a Mining Process Is Detected on a Server?

You are advised to:

1. Back up data and disable unnecessary ports.
2. Set a stronger server password.
3. Enabled HSS. Your servers will be protected from mining processes by its intrusion detection functions, such as account cracking prevention, remote login detection, malicious program detection, and web shell detection; as well as malicious program killing and vulnerability fixing functions.

## 4.4.4 What Should I Do If I Find My Servers Attacking Others?

If your servers are launching attacks, they may be infected with Trojans. You are advised to reinstall the OS and set strong passwords to harden the servers and applications such as phpStudy and Redis. Countermeasures include:

- Set strong passwords for all accounts. Do not use default passwords or other passwords that are easy to guess.
- Configure security group policies. Set fixed access IP addresses for non-public service ports to avoid its exposure to the Internet.
- Update the system and applications, installing the latest patches in a timely manner.
- Regularly back up data.
- Delete or rename the **phpmyadmin** folder.

## 4.4.5 Why Some Attacks on Servers Are Not Detected?

- 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 Web Application Firewall and Anti-DDoS).

## 4.4.6 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

- HSS block attacking IP addresses to prevent intrusions. The blocking duration for suspicious SSH attacks is 12 hours and that for other suspicious attacks is 24 hours. 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 **Intrusions** > **Events**, click **Blocked IP Addresses,** and unblock the IP address in the displayed slide-out panel.


Copyright © Huawei Technologies Co., Ltd.

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.

## 4.4.7 Why a Blocked IP Address Is Automatically Unblocked?

If a blocked IP address does not perform brute-force attacks in the next 24 hours, the IP address will be automatically unblocked.

# 4.5 Abnormal Logins

## 4.5.1 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 4-2**.

**Table 4-2** 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.<br>**NOTICE**<br>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 this whitelist. | **Log in to the management console**. Choose **Intrusions** > **Whitelists** and click the **Login Whitelist** tab. HSS will not report brute-force alarms on whitelisted alarms. |


Copyright © Huawei Technologies Co., Ltd.

| Function | Description | How to Mask Alarm |
| --- | --- | --- |
| Remote login | Logins not from **Common Login Locations** and **Common Login IP Addresses** will trigger remote login alarms.<br>You will be informed of new IP addresses that log in to your servers. | **Log in to the management console**. Choose **Installation and Configuration** > **Security Configuration**. Add login information on the **Common Login Locations** and **Common Login IP Addresses** tabs. Whitelisted logins will no longer trigger remote login alarms. |

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

## Alarm Policies

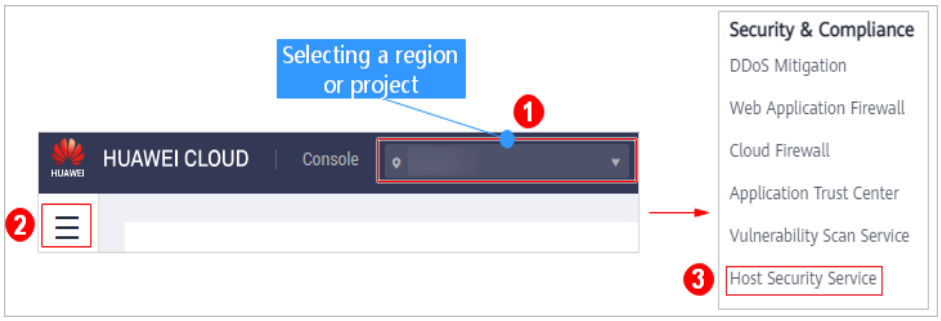
The remote login detection function checks for remote logins into your servers in real time. HSS generates an alarm if it detects logins from locations other than the **common login locations you set**.

## 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** > **Host Security Service**.

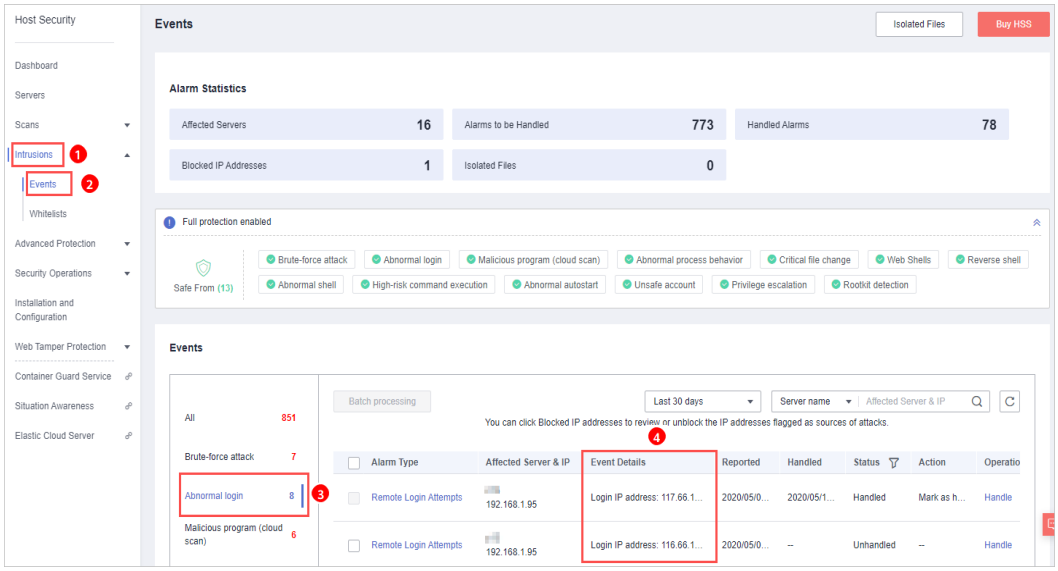
**Figure 4-22** Accessing HSS




**Step 3** Click **Abnormal login**.


Copyright © Huawei Technologies Co., Ltd.

**Figure 4-23** Remote logins




**----End**

## Locally Viewing Remote Login Records

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.

# 4.5.3 What Can I Do If an Alarm Indicating Successful Login Is Reported?

- This alarm does not necessarily indicate a security issue. If you have selected **Successful Logins** in the **Real-Time Alarm Notifications** area, HSS will send alarms when detecting any successful logins.
- If all the accounts on your 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.

# 4.5.4 Can I Disable Remote Login Detection?

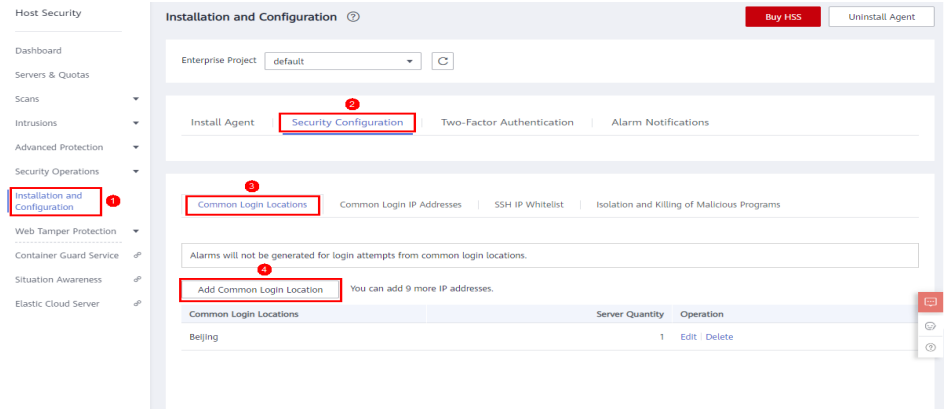
No.

If you do not want to receive remote login alarm notifications, add the locations that triggered alarms 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.

 Copyright © Huawei Technologies Co., Ltd. 

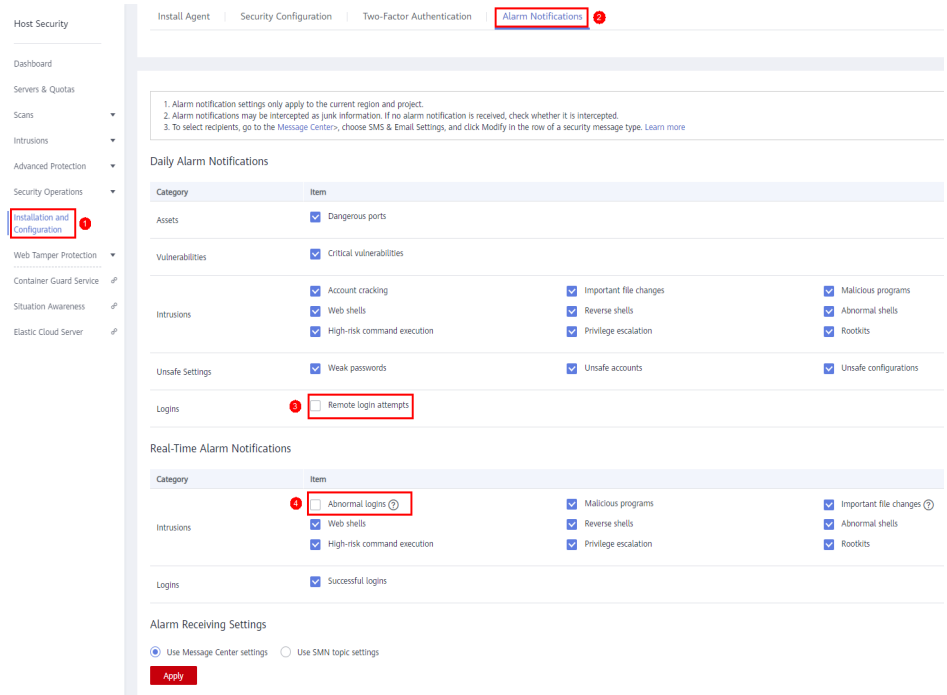
**Figure 4-24** Adding a common login location




- On the **Installation and Configuration** page, click the **Alarm Notifications** tab. Deselect **Remote Login attempts** in the **Daily Alarm Notifications** area and **Abnormal Logins** in the **Real-Time Alarm Notifications** area, as shown in **Figure 4-25**.

  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 4-25** Deselecting remote login alarm notifications




## 4.5.5 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 **Intrusion Detection** page.

 Copyright © Huawei Technologies Co., Ltd. 

- For more details, view logs in the **/var/log/secure and /var/log/message** on the Linux server, or run the **last** command to check for abnormal login records.

# 4.6 Unsafe Settings

## 4.6.1 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 in your system.

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: 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.

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 4-3**.
     Example:

 Copyright © Huawei Technologies Co., Ltd. 

password requisite pam_cracklib.so try_first_pass retry=3 minlen=9 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 type=

NOTE

At least three of **dcredit**, **ucredit**, **lcredit**, and **ocredit** must be set to negative numbers.

**Table 4-3** Parameter description

| Parameter | Description | Example |
| --- | --- | --- |
| minlen | Minimum length of a password.<br>A PAM uses **credits** by default. As a result, the minimum password length is one plus. For example, if you want the minimum length to be eight, set the **minlen** value to **9**. | minlen=9 |
| dcredit | Number of digits<br>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<br>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<br>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<br>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**

 Copyright © Huawei Technologies Co., Ltd. 

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 4-3**.

   Example:

   password requisite pam_cracklib.so retry=3 minlen=9 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 difok=3

## 4.6.2 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:

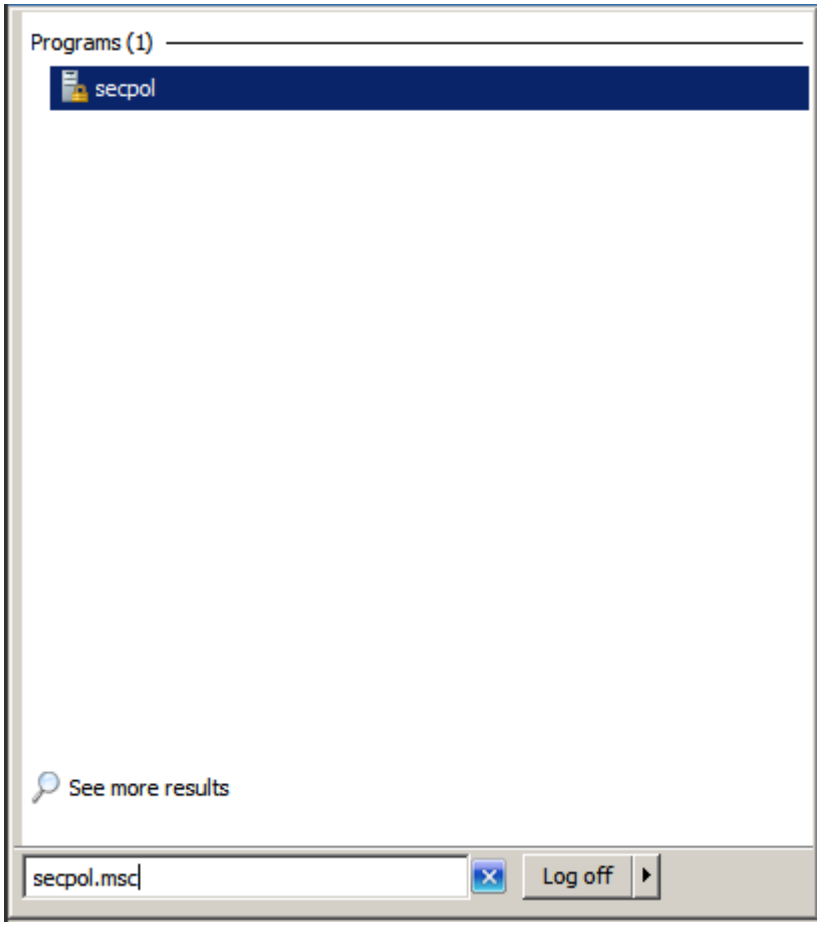
**Step 1** Log in to the OS as user **Administrator**. Choose **Start** > **Control Panel** > **System and Security** > **Administrative Tools**. In the **Administrative Tools** folder, double-click **Local Security Policy**.

NOTE

Alternatively, click **Start** and type **secpol.msc** in the **Search programs and files** box, as shown in **Figure 4-26**.


Copyright © Huawei Technologies Co., Ltd.

**Figure 4-26** Using the search box

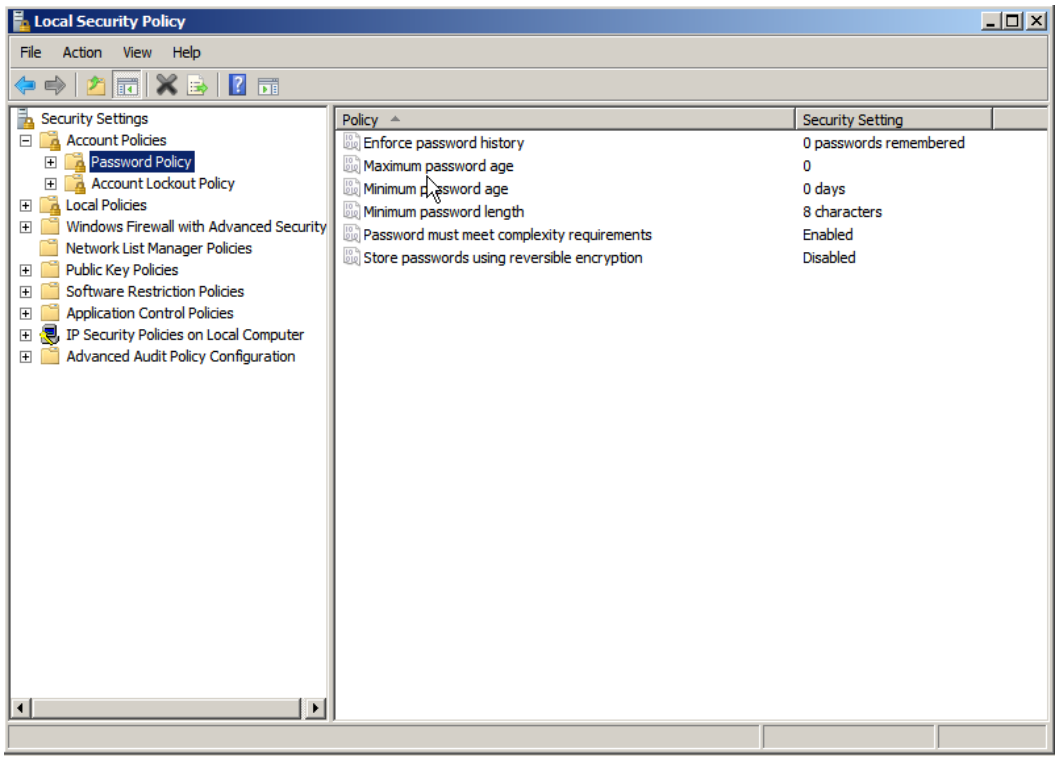



**Step 2** Choose **Account Policies** > **Password Policy** and perform the following operations, as shown in **Figure 4-27**.

- 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.

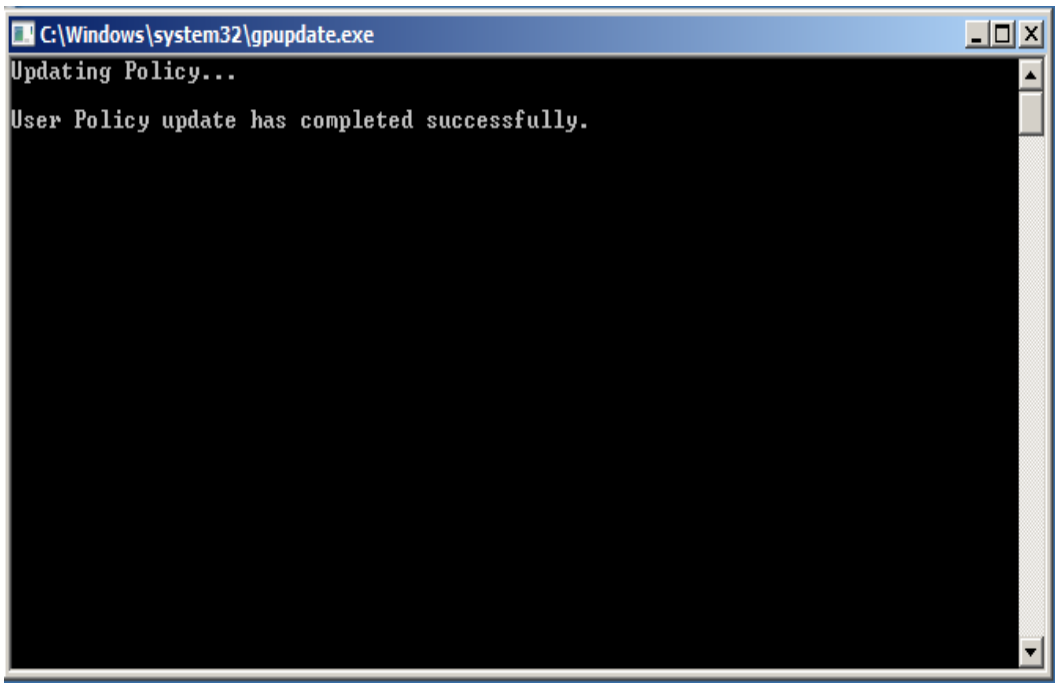

Copyright © Huawei Technologies Co., Ltd.

**Figure 4-27** Configuring local security policies




**Step 3** Run the **gpupdate** command to refresh your system settings. **Figure 4-28** shows that the refresh is successful and the settings are applied in the system.

**Figure 4-28** Execution result




**----End**


Copyright © Huawei Technologies Co., Ltd.

## 4.6.3 How Do I Handle Unsafe Configurations?

The HSS service automatically performs a configuration detection for servers. You can repair risky 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. Click the server name to view its details.

  b. Select a risky detection rule and click **Ignore** in the **Operation** column or **Ignore** in the upper left corner above the detection rule list. You can also select multiple detection rules and click **Ignore** in the upper left corner above the detection rule list to batch ignore them, as shown in **Figure 4-29**.

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

  **Figure 4-29** Batch ignoring detection rules




- Verification

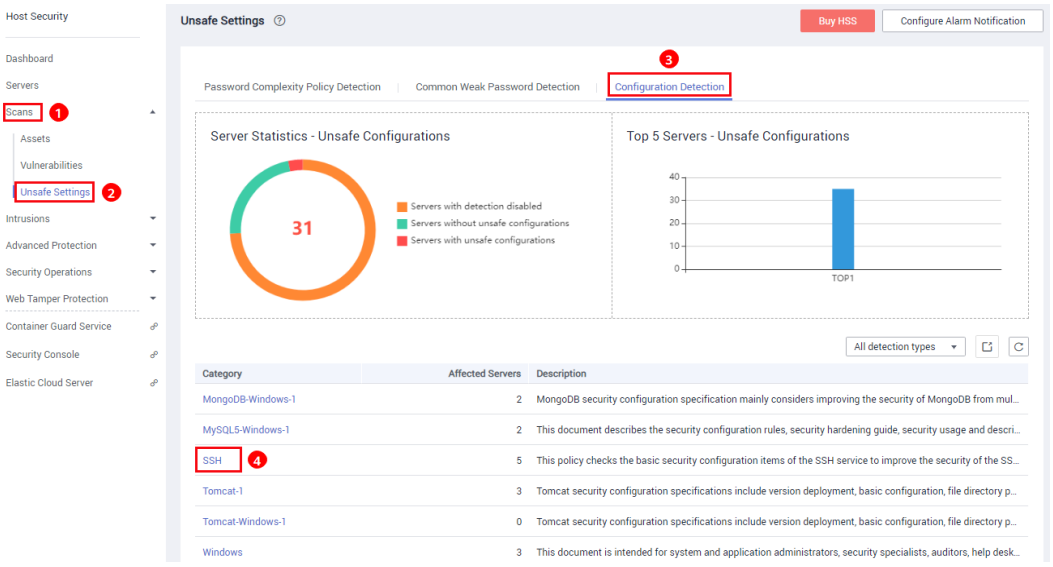
  After the configuration items are recovered, you are advised to **start a manual detection** to verify the result.

## 4.6.4 How Do I View Configuration Check Reports?

### Procedure

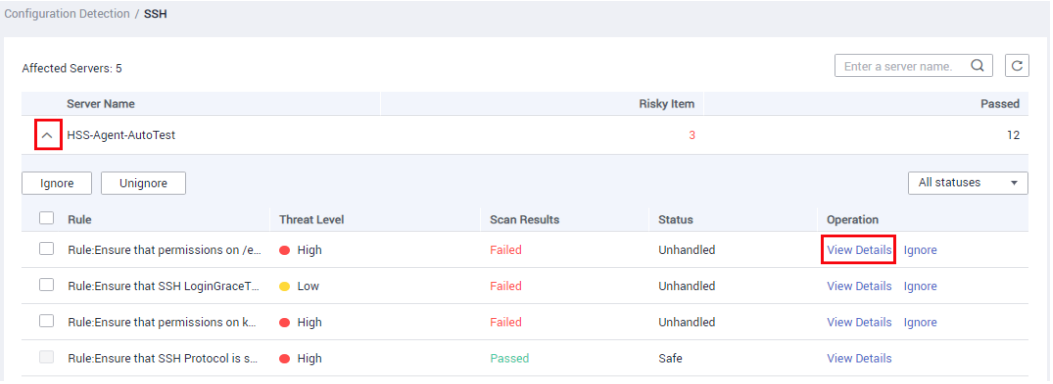
**Step 1** On the **Configure Detection** page, click a check item, for example, **SSH**.

**Figure 4-30** Choosing a check item




**Step 2** On the detection rule details page, click **View Details**.

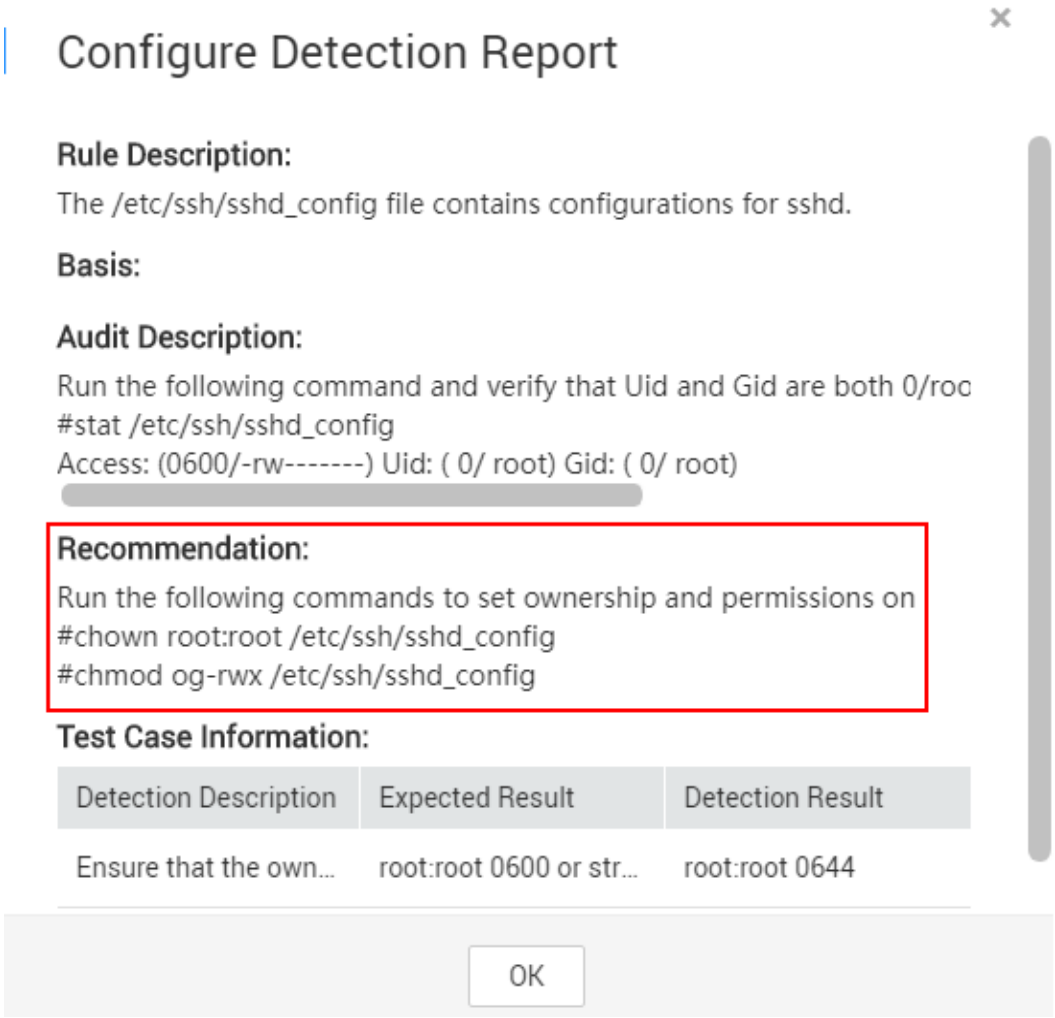
**Figure 4-31** Detection details




**Step 3** You can rectify unsafe configuration items and ignore trusted configuration items based on the suggestions provided.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 4-32** Configuring the detection report




**----End**

## 4.6.5 Do I Need to Handle Detected Configuration Problems of the Windows OS?

Yes. Modify risky configuration items based on the rectification suggestions.

For details, see **Suggestions on Fixing Unsafe Settings**.

 Copyright © Huawei Technologies Co., Ltd. 

# 5 Vulnerability Management

## 5.1 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, Windows, 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. For details, see **Starting a Software Vulnerability Detection**.

**----End**

### Helpful Links

**How Do I Handle Unsafe Configurations?**

## 5.2 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 more information, see **Fixing Vulnerabilities and Verifying the Result**.

### Possible Causes and Solutions on a Windows Server

- The patch package failed to be downloaded.

 Copyright © Huawei Technologies Co., Ltd. 

Your server may not have the permission to access the Internet. In this case, connect to the Internet and fix the vulnerability again.

- The patch package does not match your OS.

  In this case, select the vulnerability and click **Ignore** on the **Vulnerabilities** page.

- Another patch is being installed.

  In this case, wait until the current patch is installed, and then fix the vulnerability.

- Server settings hinder vulnerability fix or alarm clearance.
  - If automatic patch update is enabled on the server, and you have confirmed that a patch has been installed to fix the vulnerability, you can ignore the vulnerability on the console.
  - If the latest patch has overwritten old patches (in Windows Server 2016 and later), and you have confirmed that a patch has been installed to fix the vulnerability, you can ignore the vulnerability on the console.
  - If a piece of security software (such as the Server Edition of 360 Guard) blocks the vulnerability patch, stop the software, fix the vulnerability, and then start the software again.

**NOTICE**

- Microsoft has stopped updating and maintaining Windows Server 2008 R2 since January 14, 2020. To continue to use the system, you need to purchase Extended Security Update (ESU) keys and activate or replace the Windows OS.

## 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.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 5-1** Verification commands

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

### Follow-up Operations

After the vulnerability is fixed, you are advised to perform a manual detection to verify the result. For details, see **How Do I Scan My Servers?**

NOTE

- HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.
- Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

## 5.3 Why a Server Displayed in Vulnerability Information Does Not Exist?

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

## 5.4 Do I Need to Restart a Server After Fixing its Vulnerabilities?

- On a Windows server, you need to restart it after you fix its vulnerabilities.
- On a Linux server, you need to restart it after you fixed a kernel vulnerability. Restart is not required for other vulnerability fixes.

## 5.5 How Do I Check Vulnerability Severity?

Check the **Urgency** column on the **Vulnerabilities** page.

The urgency of a vulnerability indicates its severity.

- **High**: This is a high-risk vulnerability and must be fixed as soon as possible. Attackers may exploit this vulnerability to damage the server.


Copyright © Huawei Technologies Co., Ltd.

- **Medium**: This is a medium-risk vulnerability and you are advised to fix the vulnerability to enhance your server security.
- **Safe for now**: This is a low-risk vulnerability and has a small threat to server security. You can choose to fix or ignore it.

  NOTE

  On the **Vulnerabilities** page, you can **check vulnerability details**, **fix vulnerabilities, and verify the result**.

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

No.

You can check and export existing vulnerability information and vulnerability scan reports. For details, see **Viewing Details of a Vulnerability**.

You can also check and export existing baseline details and baseline scan reports. For details, see **Checking for Unsafe Settings**.


Copyright © Huawei Technologies Co., Ltd.

# 6 Web Tamper Protection

## 6.1 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.

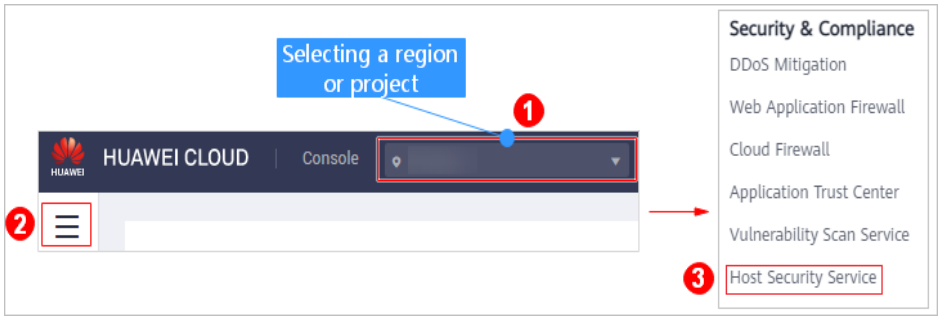
For details, see **Enabling WTP**.

## 6.2 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** > **Host Security Service**.

**Figure 6-1** Accessing HSS




**Step 3** In the navigation pane, choose **Web Tamper Protection** > **Server Protection**.

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

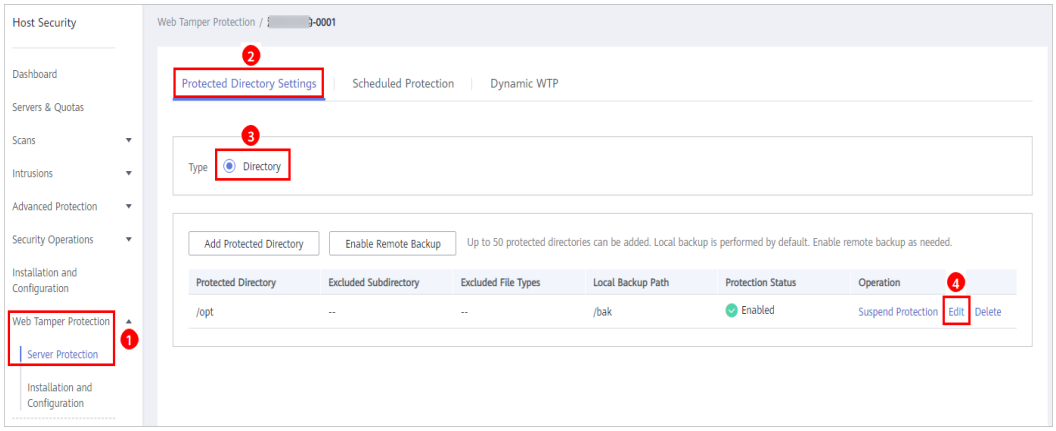
**Step 5** Select the required protected directory and click **Edit** in the **Operation** column.

 Copyright © Huawei Technologies Co., Ltd. 

**NOTE**

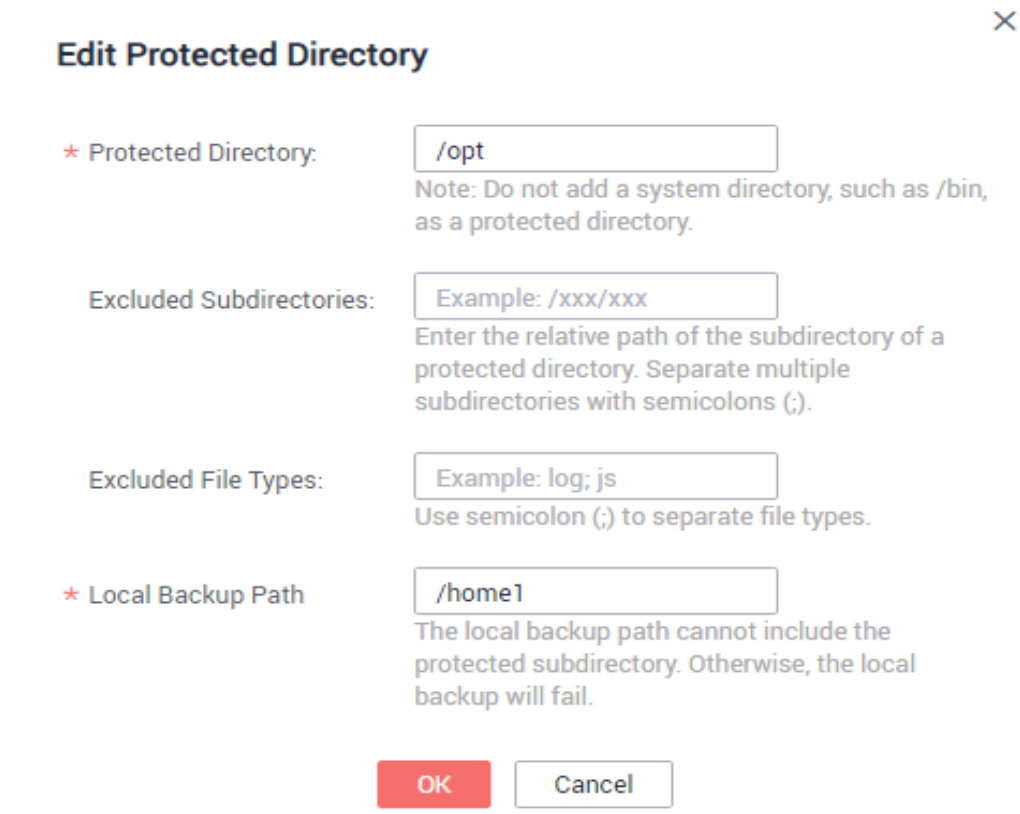
- If you need to modify files in the protected directory, stop protection for the protected directory first.
- After the files are modified, resume protection for the directory in a timely manner.

**Figure 6-2** Configuring protection




**Step 6** In the **Edit Protected Directory** dialog box, modify the settings and click **OK**.

**Figure 6-3** Editing protected directory




**----End**

 Copyright © Huawei Technologies Co., Ltd. 

# 6.3 What Should I Do If WTP Cannot Be Enabled?

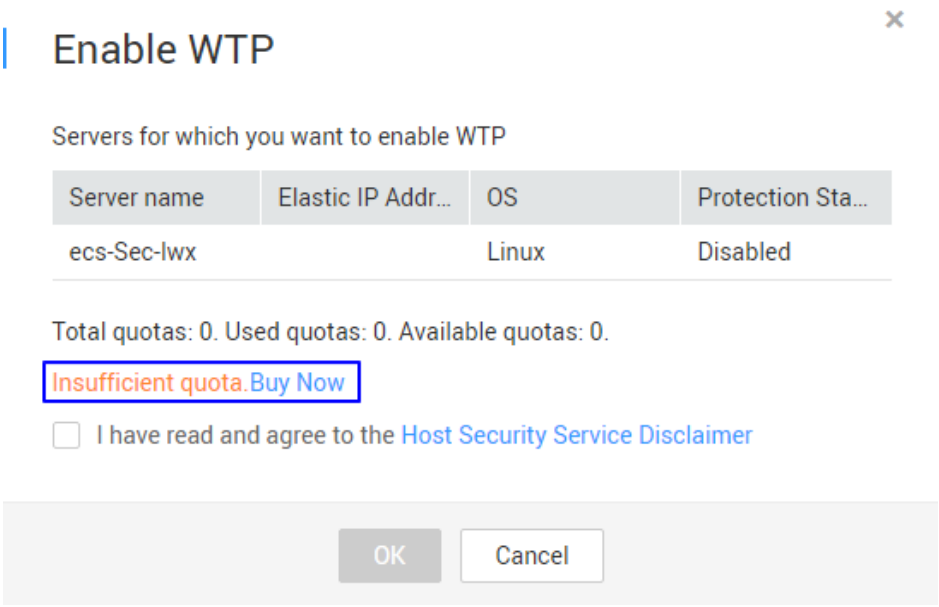
The causes of this problem vary by scenarios.

## Insufficient Quota

- **Symptom**

  The WTP quota in the selected region is insufficient, as shown in **Figure 6-4**.

  **Figure 6-4** Insufficient quota




- **Solution**

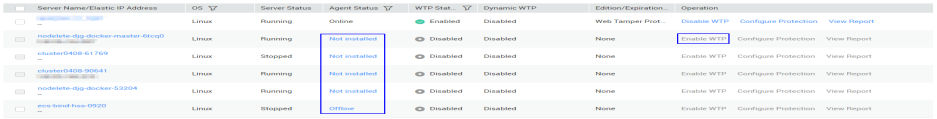
  **Purchase WTP quota** in the selected region.

## Agent Status Is Abnormal

- **Symptom**

  The agent status is **Offline** or **Not installed** in the **server list** on the **Web Tamper Protection** page, as shown in **Figure 6-5**.

  **Figure 6-5** Agent status



- **Solution**

  Rectify the fault by following the instructions provided in **What Should I Do When the Agent Running Status Is Abnormal?**. Ensure that **Agent Status** in the server list is **Online**.

 Copyright © Huawei Technologies Co., Ltd. 

## Basic or Enterprise 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**.

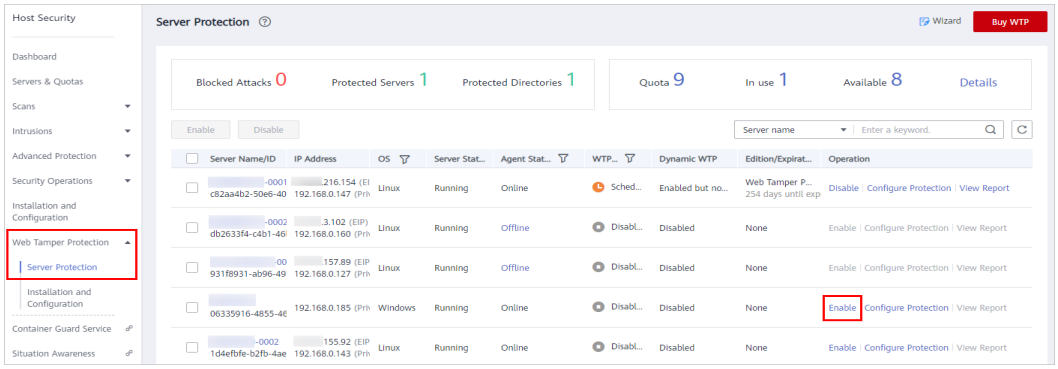
  NOTE

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

## Protection Was Enabled on the Wrong Page

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

**Figure 6-6** Web Tamper Protection




NOTE

If you have purchased 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.

# 6.4 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.

## Specifying Privileged Processes

Privileged processes have the permission to modify files. For details, see **Adding a Privileged Process That Can Modify Protected Files**.

- Privileged processes can access protected directories. Ensure that privileged processes are secure and reliable.
- You can configure privileged processes only for Windows OSs.

## Temporarily Disabling WTP

Disable WTP while you modify files in protected directories.


Copyright © Huawei Technologies Co., Ltd.

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.

## 6.5 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.

## 6.6 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 WTP

**Table 6-1** describes the differences

 Copyright © Huawei Technologies Co., Ltd. 

**Table 6-1** Differences between the web tamper protection functions of HSS and WTP

| Item | HSS | WAF |
| --- | --- | --- |
| Static web page protection | Locks files in driver and web file directories to prevent attackers from tampering with them. | Caches static web pages on servers. |
| Dynamic web page protection | • Dynamic WTP<br>Protects your data while Tomcat is running, detecting dynamic data tampering in databases.<br>• Privileged process management<br>Allows privileged processes to modify web pages. | No |
| Backup and restoration | • Active backup and restoration<br>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.<br>• Remote backup and restoration<br>If a file directory or backup directory on the local server becomes invalid, you can use the remote backup service to restore the tampered web page. | No |
| Suitable for | Websites that have high security requirements and difficult to be manually recovered | Websites that only require application-layer protection |

## Purchase Suggestion

| 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 |

 Copyright © Huawei Technologies Co., Ltd. 

# 7 Enterprise Project

## 7.1 How Do I Migrate Settings Between Projects After Enabling Enterprise Projects for HSS?

HSS now supports enterprise projects.

Before HSS supports the enterprise project function, if you put your servers under different enterprise projects in other services, all the ECSs would be put in the **default** project in HSS by default.

Now in HSS, servers will be automatically put under their corresponding enterprise projects, but the enterprise projects will not inherit the settings of the **default** project. You need to manually configure the enterprise projects again or contact technical support to migrate the **default** project settings to the enterprise projects.

**NOTICE**

- Mandatory settings: alarm notifications
- Optional settings: security settings, server groups, whitelist, file integrity monitoring (FIM), security reports, remote backup servers, and migration quotas

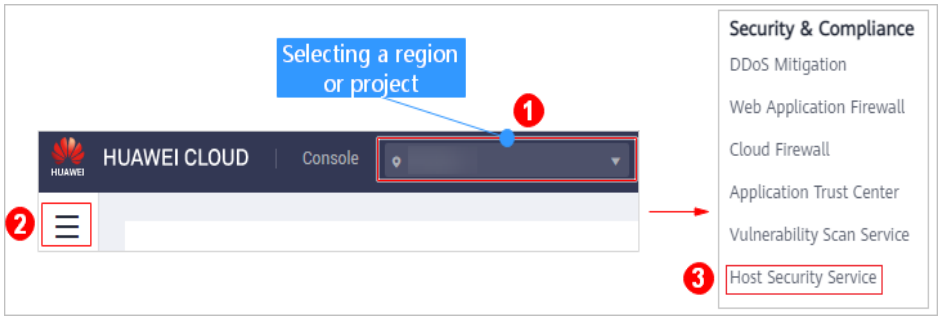
The following procedure takes the **default** project and **Enterprise Project 1** as examples.

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

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

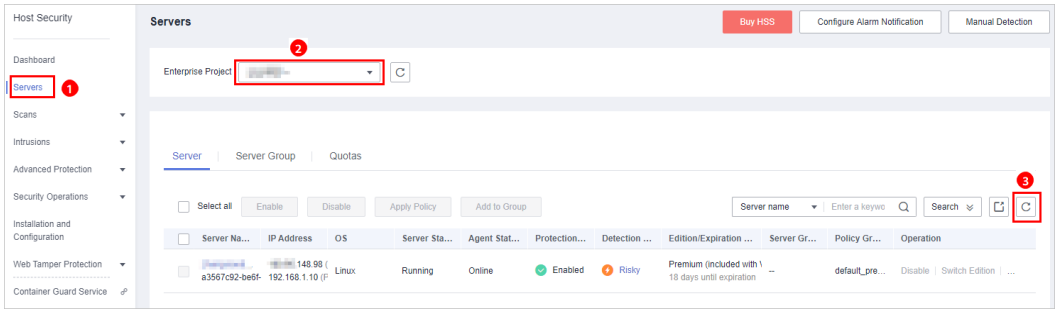
 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-1** Accessing HSS




**Step 3** On the **Servers** page, select **Enterprise Project 1** from the **Enterprise Project** drop-down list, and refresh the server list, as shown in **Figure 7-2**.

**Figure 7-2** Refreshing the server list



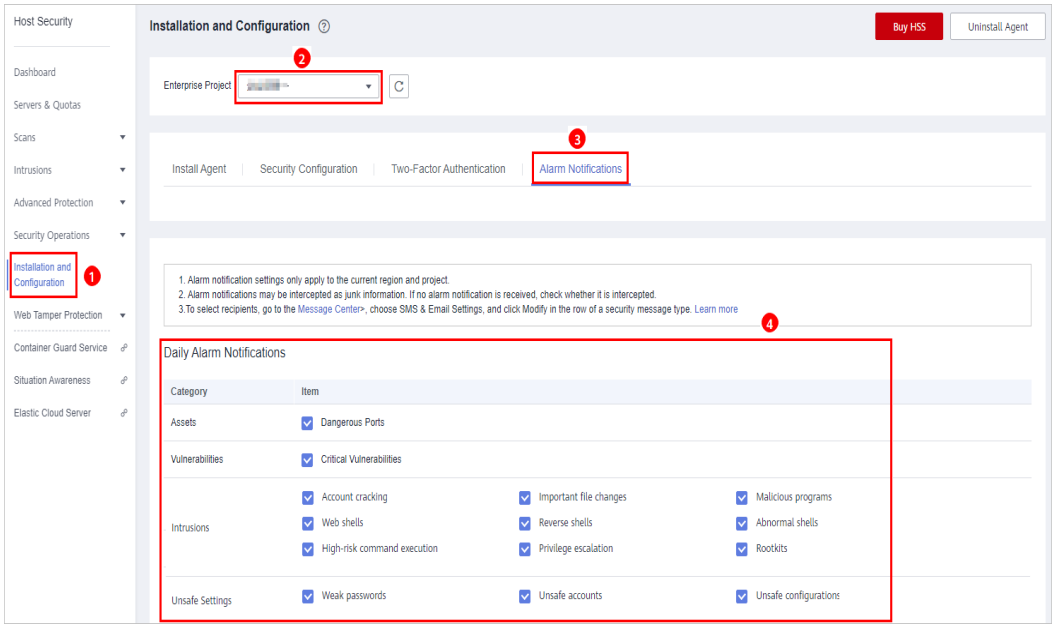

**----End**

## (Mandatory) Configuring Alarm Notifications

- Configuring alarm notification for the basic, enterprise, or premium edition

**Step 1** Open the **Alarm Notifications** tab, as shown in **Figure 7-3**.

**Figure 7-3** Basic/Professional/Premium edition




 Copyright © Huawei Technologies Co., Ltd. 

**Step 2** Select the notification items for **Daily Alarm Notifications** and **Real-Time Alarm Notifications** as desired.

**Step 3** Select **Use Message Center settings** or **Use SMN topic settings**.

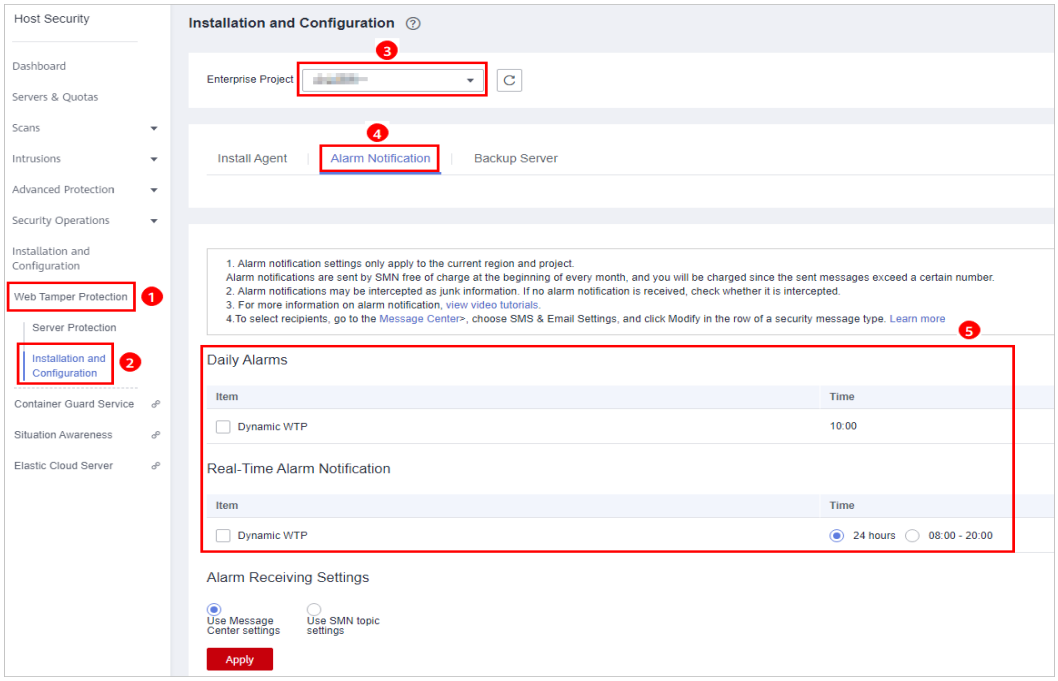
**Step 4** Click **Apply**. A message will be displayed indicating that the alarm notification is set successfully.

**----End**

- Configuring WTP alarm notifications

**Step 1** Configure alarm time on the **Alarm Notifications** tab, as shown in **Figure 7-4**.

**Figure 7-4** Configuring alarm notifications




**Step 2** Select the notification items for **Daily Alarm Notifications** and **Real-Time Alarm Notifications** as desired.

**Step 3** Select **Use Message Center settings** or **Use SMN topic settings**.

**Step 4** Click **Apply**. A message will be displayed indicating that the alarm notification is set successfully.

**----End**

## (Optional) Migrating Security Settings

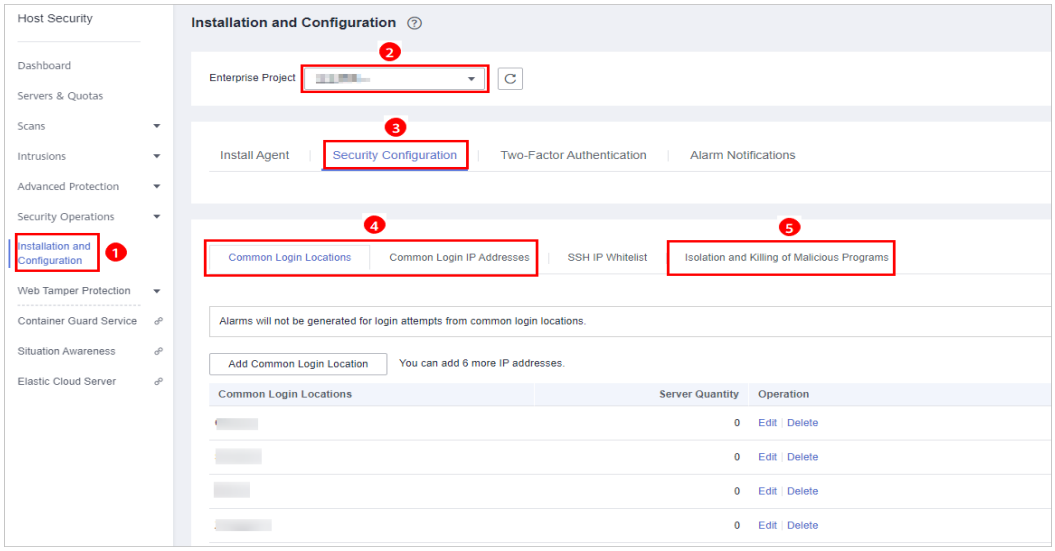
Configure your enterprise project security settings, including common login locations, common login IP addresses, and the automatic isolation and killing of malicious programs.

After enterprise projects are supported, the SSH login IP address whitelist will be automatically migrated from the **default** project to **Enterprise Project** 1.

 Copyright © Huawei Technologies Co., Ltd. 

On the **Installation and Configuration** page, click the **Security Configuration** tab. Configure common login locations, common login IP addresses, and the automatic isolation and killing of malicious programs, as shown in **Figure 7-5**.

**Figure 7-5** Configuring security settings

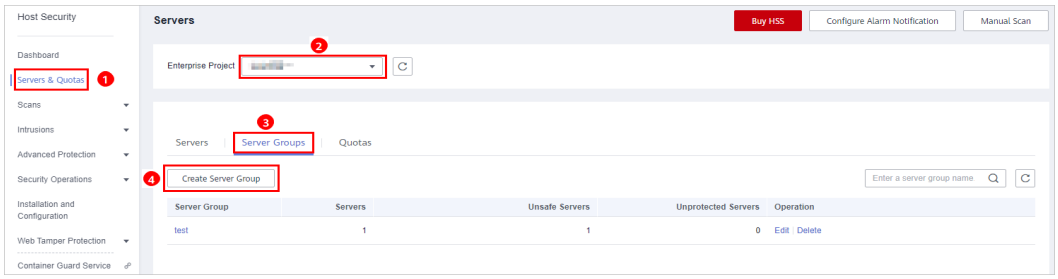



## (Optional) Creating Server Groups

Create server groups under an enterprise project.

**Step 1** Choose **Servers**, and click the **Server Group** tab. Click **Create Server Group**, as shown in **Figure 7-6**.

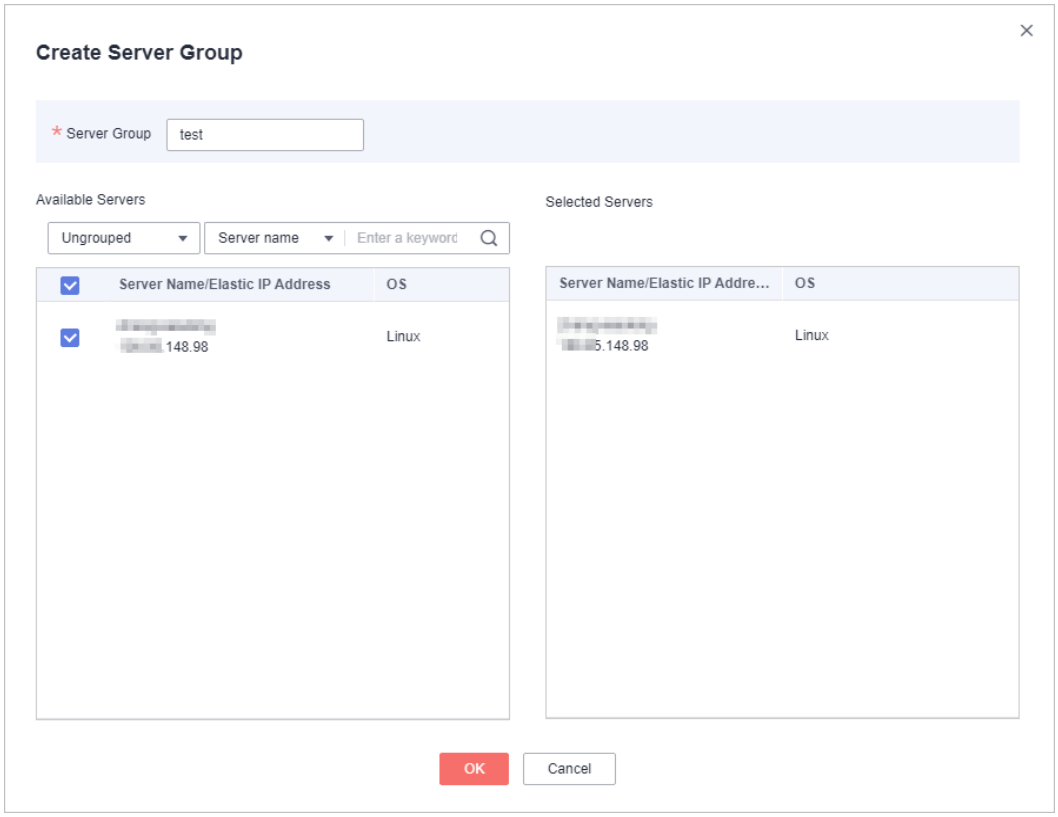
**Figure 7-6** Accessing the Server Group tab




**Step 2** In the displayed **Create Server Group** dialog box, set the server group name and add servers to the group, as shown in **Figure 7-7**.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-7** Assigning servers




**Step 3** Click **OK**.

**----End**

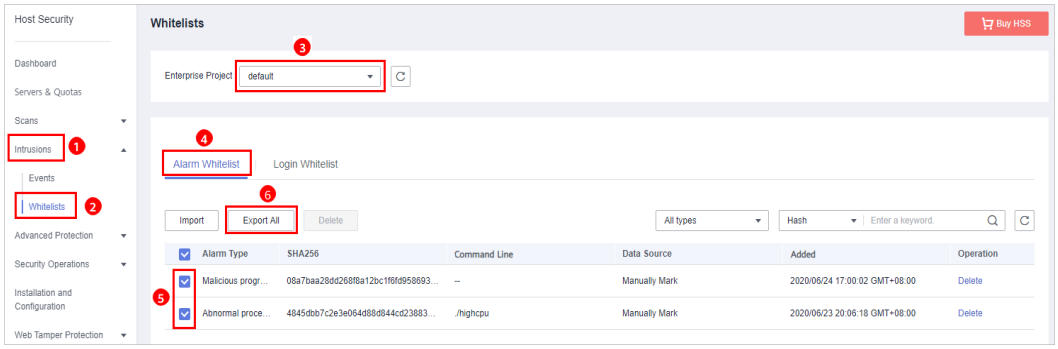
## (Optional) Migrating Whitelist Data

Manually migrate alarm and login whitelist settings to enterprise projects.

- To migrate the alarm whitelist, manually export the alarm whitelist from the **default** project and then it to **Enterprise Project 1**.
- To migrate the login whitelist, manually configure it for **Enterprise Project 1**.

**Step 1** Chooses **Intrusions** > **Whitelists**, select the **default** project, and export its alarm whitelist, as shown in **Figure 7-8**.

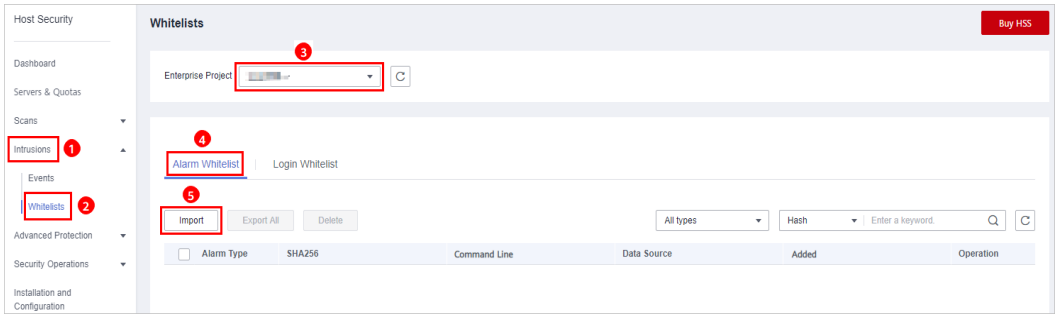
**Figure 7-8** Exporting the alarm whitelist




 Copyright © Huawei Technologies Co., Ltd. 

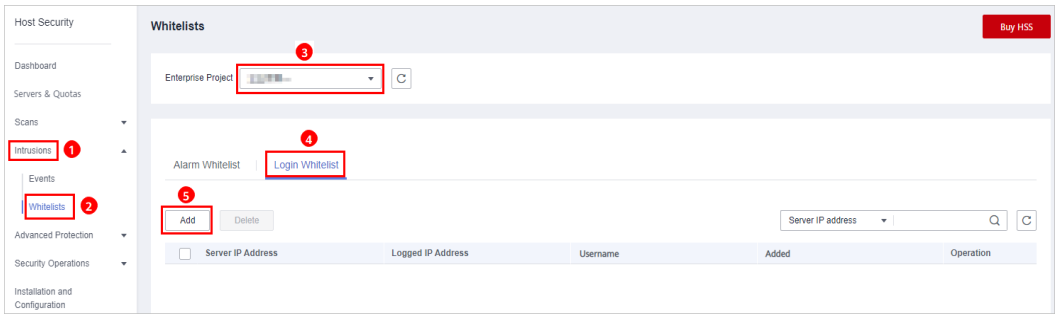
**Step 2** Select **Enterprise Project 1** from the **Enterprise Project** drop-down list and import the alarm whitelist, as shown in **Figure 7-9**.

**Figure 7-9** Importing the alarm whitelist




**Step 3** Configure the login whitelist on the **Login Whitelist** tab, as shown in **Figure 7-10**.

**Figure 7-10** Configuring the login whitelist



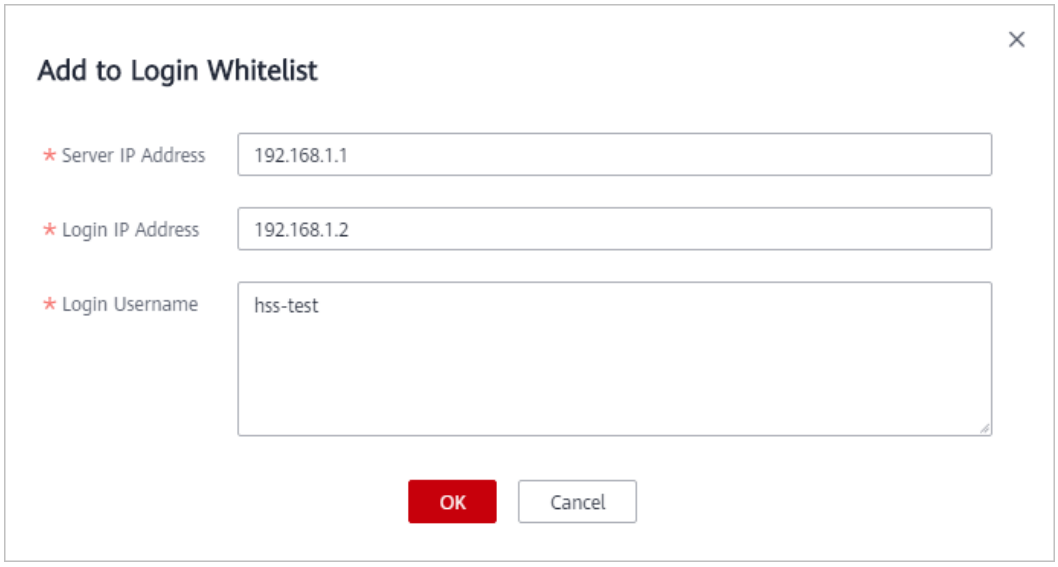

**Step 4** In the **Add to Login Whitelist** dialog box, enter the server IP address, login IP address, and login username, as shown in **Figure 7-11**.

NOTE

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


Copyright © Huawei Technologies Co., Ltd.

**Figure 7-11** Adding login information to the login whitelist




**Step 5** Click **OK**.

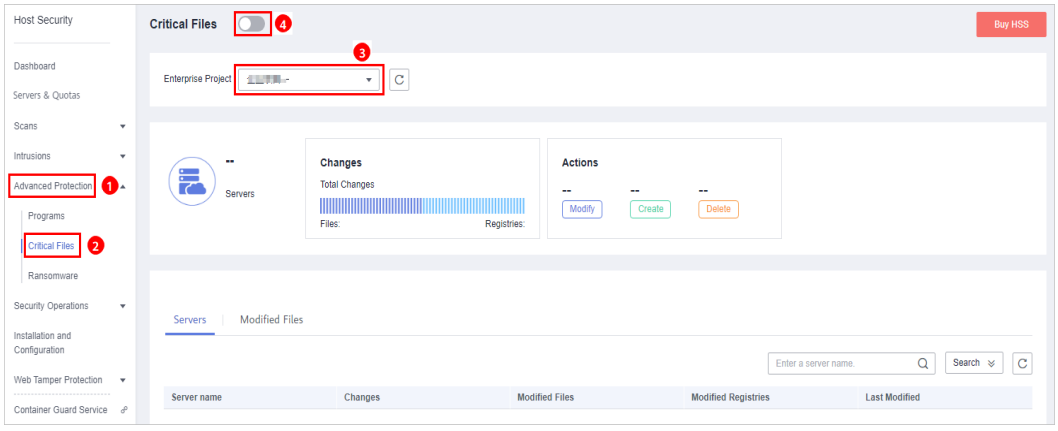
**----End**

## (Optional) Enabling FIM

If you are using the premium edition, you can manually enable FIM for enterprise projects.

On the **Critical Files** page, click  to enable FIM, as shown in **Figure 7-12**.

**Figure 7-12** Enabling FIM

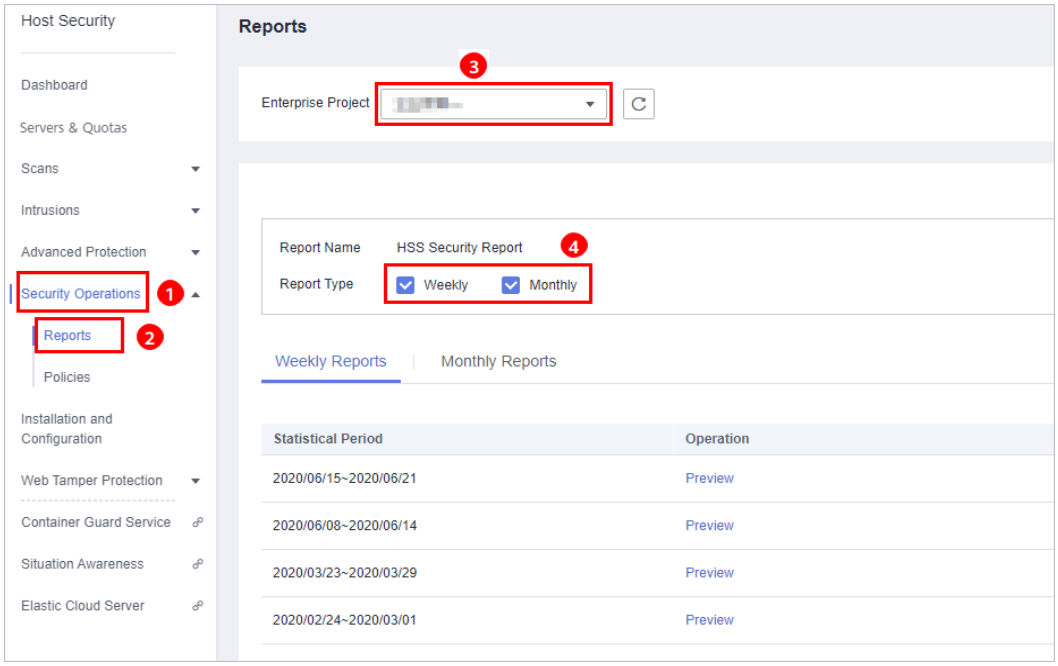



## (Optional) Subscribing to Security Reports

Choose **Security Operations** > **Reports** and select **Weekly** and **Monthly**, as shown in **Figure 7-13**.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-13** Subscribing to security reports

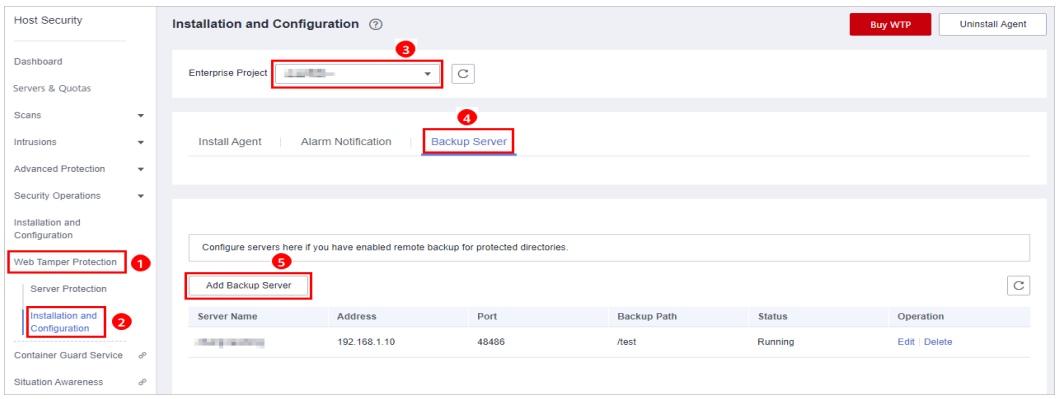



## (Optional) Configuring a Remote Backup Server for Web Tamper Protection

Configure a remote backup server for **Enterprise Project 1** and enable remote backup.

**Step 1** Choose **Web Tamper Protection** > **Installation and Configuration** and add a remote backup server, as shown in **Figure 7-14**.

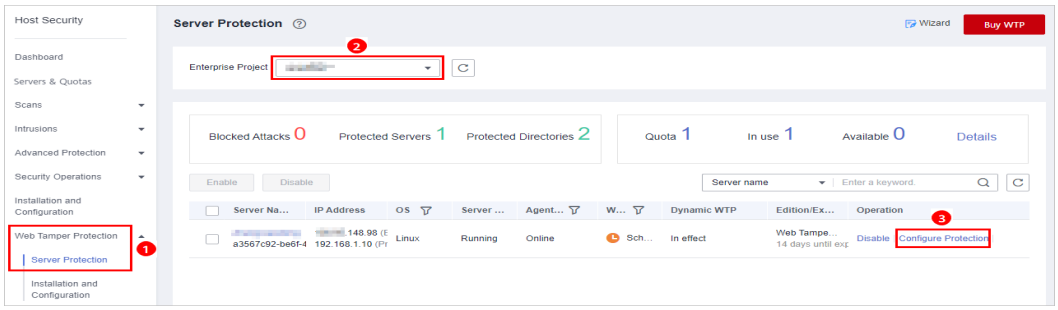
**Figure 7-14** Adding a remote backup server




**Step 2** On the **Server Protection** page, click **Configure Protection**, as shown in **Figure 7-15**.

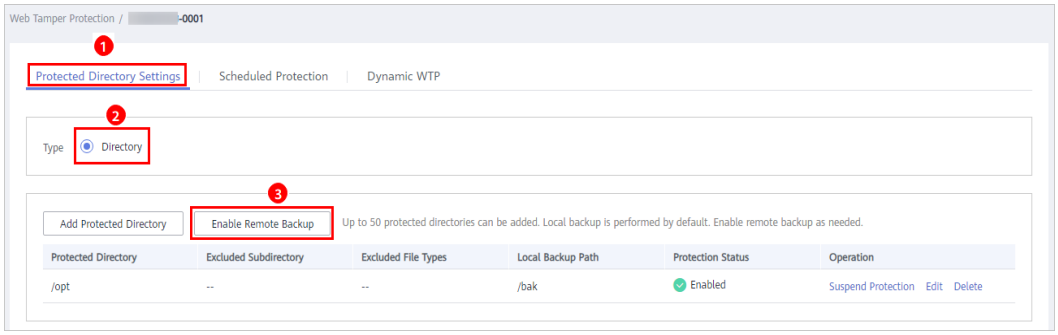

Copyright © Huawei Technologies Co., Ltd.

**Figure 7-15** Server Protection page




**Step 3** On the **Protected Directory Settings** tab, enable remote backup, as shown in **Figure 7-16**.

**Figure 7-16** Enabling remote backup




**Step 4** In the **Enable Remote Backup** dialog box, select a remote backup server from the drop-down list and click **OK**.

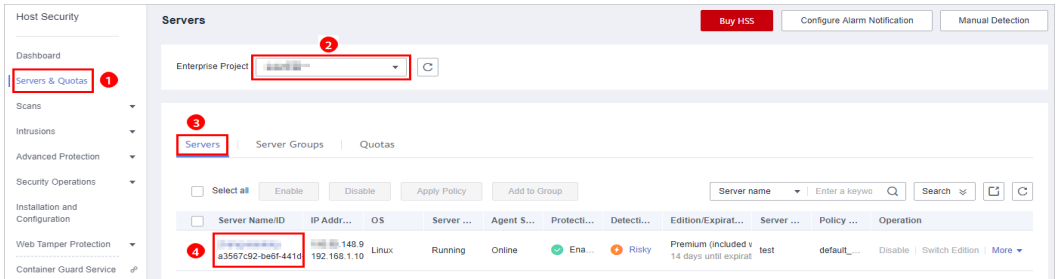
**----End**

## (Optional) Migrating Quotas

If servers protected by the HSS quotas of the **default** project are moved to **Enterprise Project 1**, and HSS is disabled for the servers, the servers can no longer use yearly/monthly quotas of the **default** project. In this case, you can migrate quotas from the **default** project to **Enterprise Project 1**. Perform the following steps:

**Step 1** Choose **Servers**, select **Enterprise Project 1** from the **Enterprise Project** drop-down list, and obtain the name of a server under the project, as shown in **Figure 7-17**.

**Figure 7-17** Checking the server name

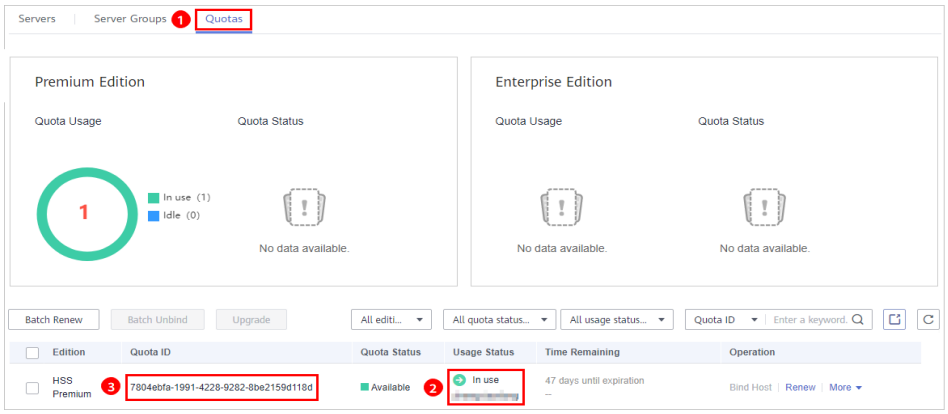



 Copyright © Huawei Technologies Co., Ltd. 

**Step 2** Obtain a quota ID.

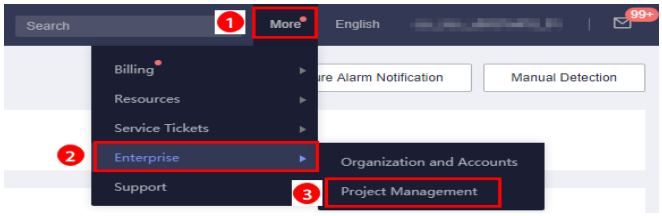
- If the **Protection Status** of the server is **Enabled**, click the **Quotas** tab, and find and record its quota ID based on the server name, as shown in **Figure 7-18**.
- If the **Protection Status** of the server is **Disabled**, click the **Quotas** tab, and find and record the ID of a quota whose status is **Idle**.

**Figure 7-18** Obtaining a quota ID



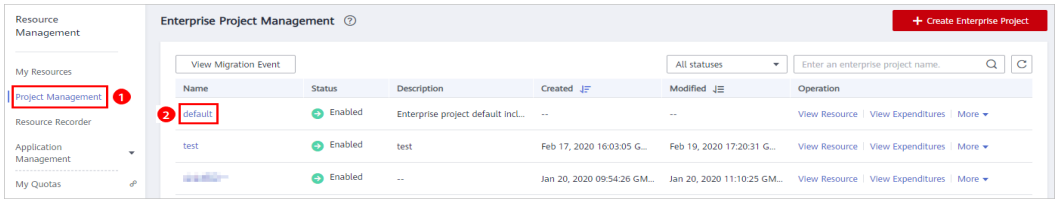

**Step 3** In the upper right corner of the console, choose **Enterprise** > **Project Management**, as shown in **Figure 7-19**.

**Figure 7-19** Choosing Project Management




**Step 4** On the **Project Management** page, click **default** to go to the project details page, as shown in **Figure 7-20**.

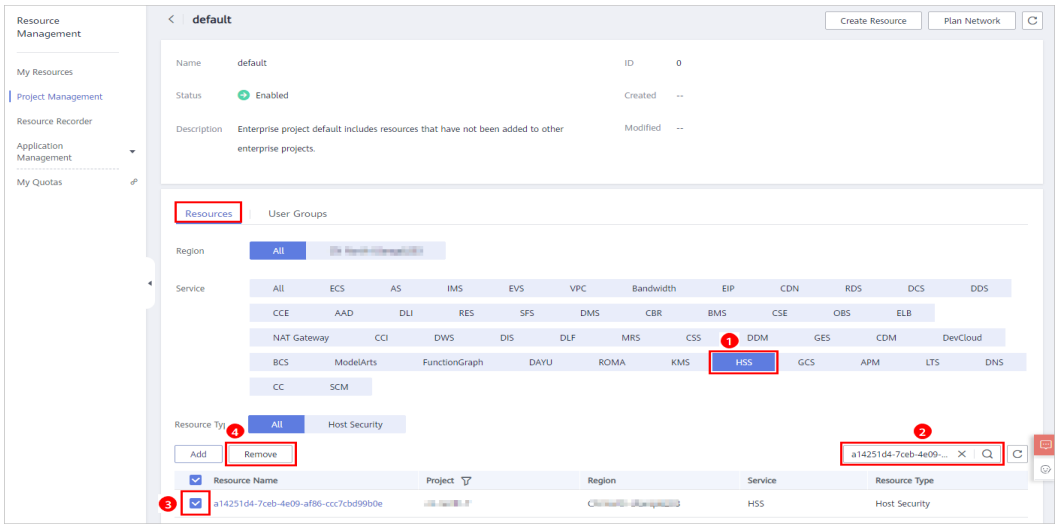
**Figure 7-20** Checking default project details




**Step 5** On the **Resources** tab, select **HSS**, find the quota by the ID obtained in **Step 2**, and remove the quota, as shown in **Figure 7-21**.

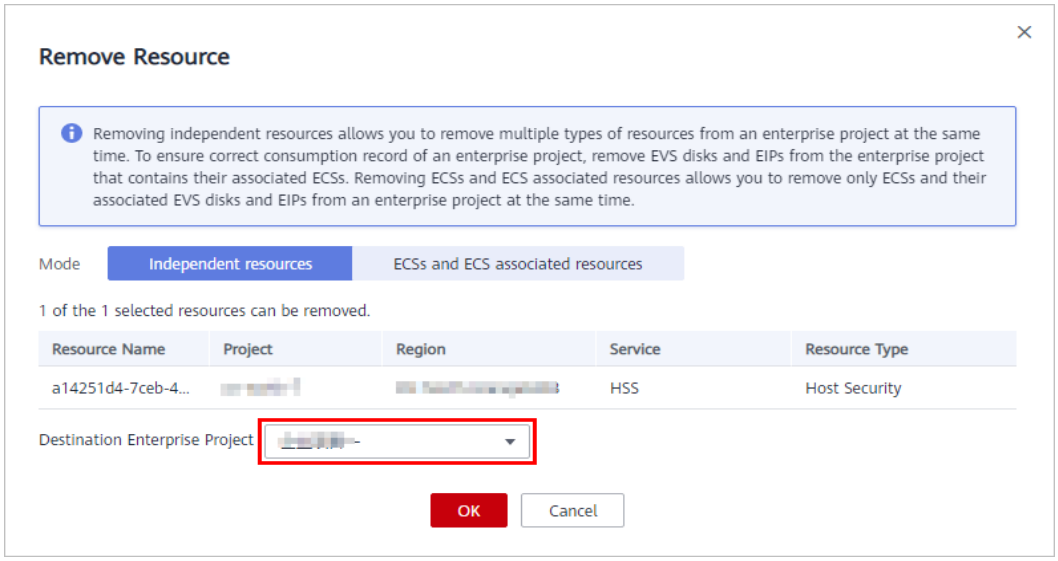

Copyright © Huawei Technologies Co., Ltd.

**Figure 7-21** Removing the quota




**Step 6** In the displayed **Remove Resource** dialog box, select the project you want to move the resource to, for example, **Enterprise Project 1**, as shown in **Figure 7-22**.

**Figure 7-22** Moving the resource to an enterprise project




**Step 7** Click **OK**. You can use the quota under the enterprise project.

To check the quota, choose **Servers**, select **Enterprise Project 1** from the **Enterprise Project** drop-down list, and click the **Quotas** tab.

**----End**

# 7.2 Can I Bind a Server to an HSS Quota If They Are in Different Enterprise Projects?

Yes. However, for convenience management purposes, you are advised to purchase quotas under the same enterprise project as your servers.

You can bind a server to a quota in either of the following ways:

 Copyright © Huawei Technologies Co., Ltd. 

- Binding a quota under **All projects**

  Under **All projects**, bind the server to the quota across enterprise projects. The project that the quota belongs to will be billed for the quota.

- Migrating a quota

  Migrate the quota to the enterprise project of the server and then bind the server to the quota.

## Binding a Quota Under All projects

### Prerequisite

You have the **Tenant Administrator** or **HSS Administrator+Tenant Guest** permissions.

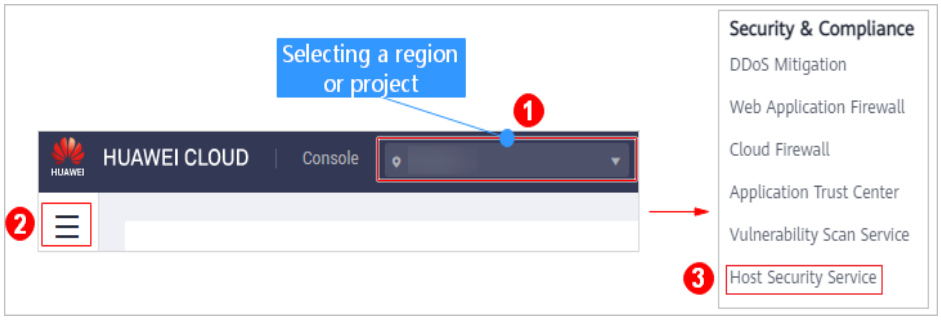
### Procedure

Perform the following steps to bind a premium edition quota to a server under **All projects**.

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

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

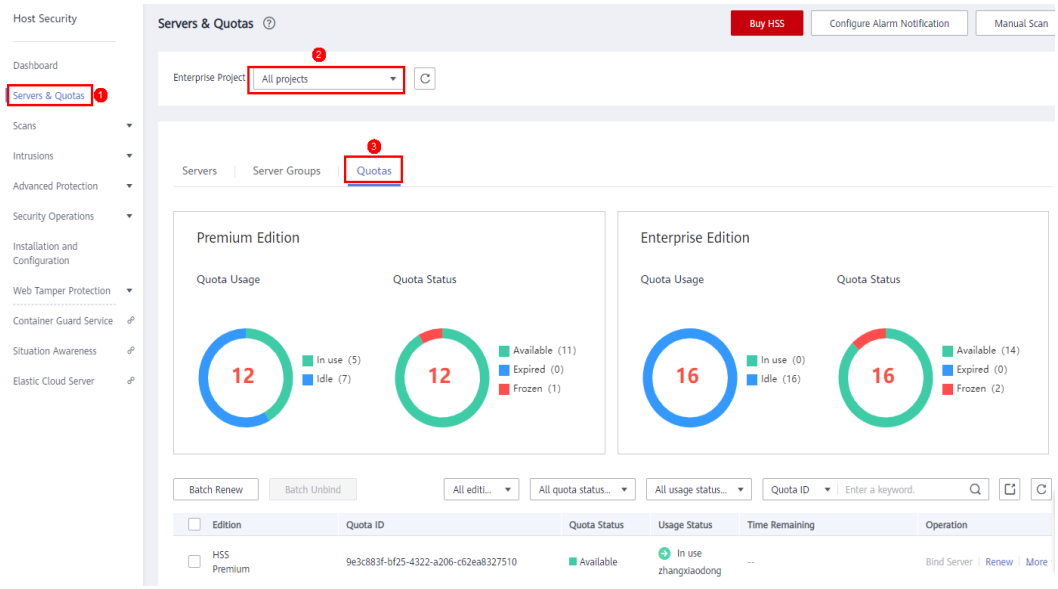
**Figure 7-23** Accessing HSS




**Step 3** Choose **Servers** and select **All projects** from the **Enterprise Project** drop-down list. Click the **Quotas** tab.

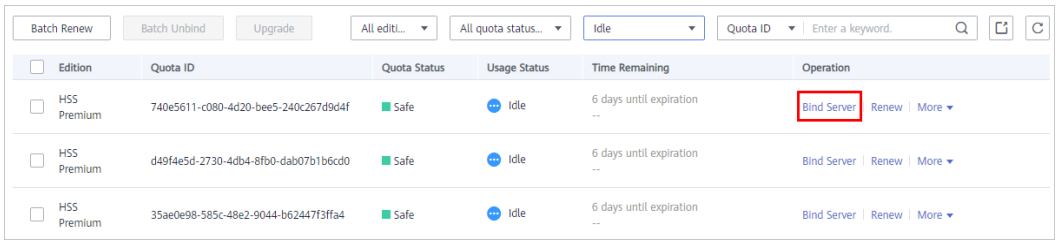

Copyright © Huawei Technologies Co., Ltd.

**Figure 7-24** Protection quotas




**Step 4** In the quota list, select a quota whose **Usage Status** is **Idle** and click **Bind Server**.

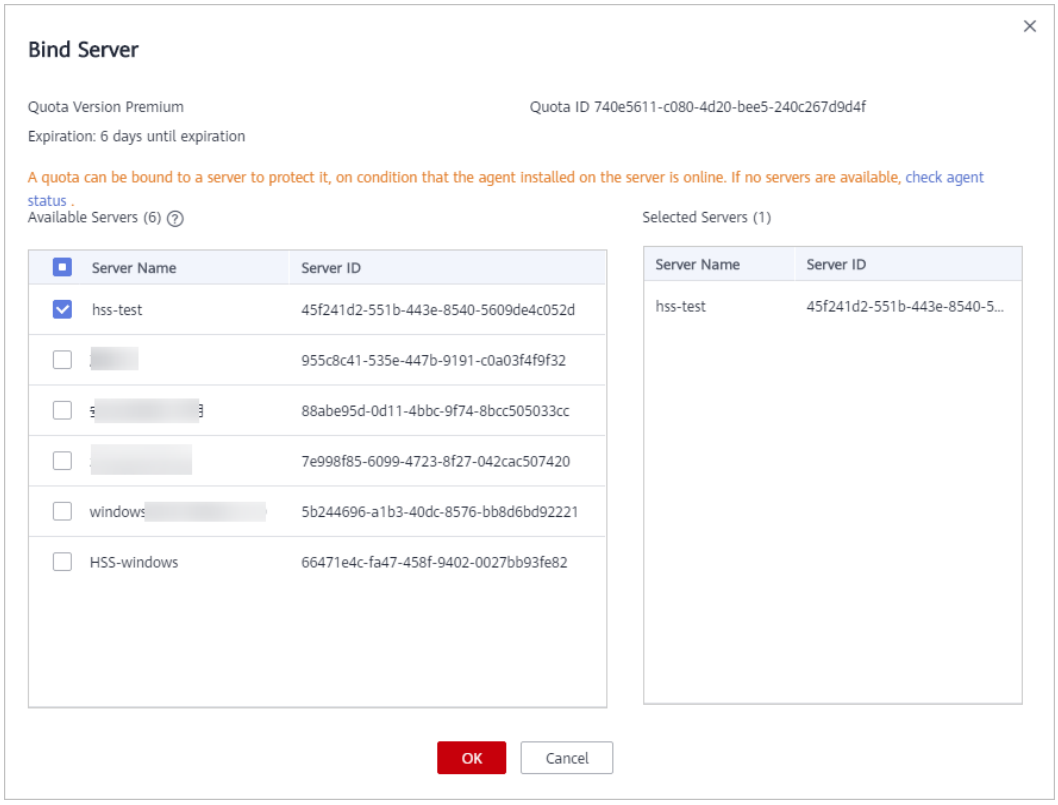
**Figure 7-25** Binding a quota to a server




**Step 5** Select servers in the **Details** dialog box.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-26** Binding a quota




**Step 6** Click **OK**. The **Protection Status** of the server will change to **Enabled**.

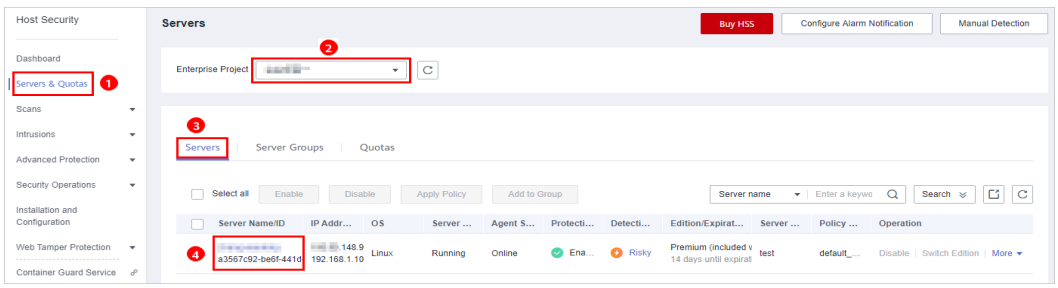
**----End**

## Migrating a Quota

Assume all the quotas belong to the **default** project. You can perform the following steps to migrate a quota to **Enterprise Project 1** and bind it to a server.

**Step 1** Choose **Servers**, select **Enterprise Project 1** from the **Enterprise Project** drop-down list, and obtain the name of a server under the project, as shown in **Figure 7-27**.

**Figure 7-27** Checking the server name



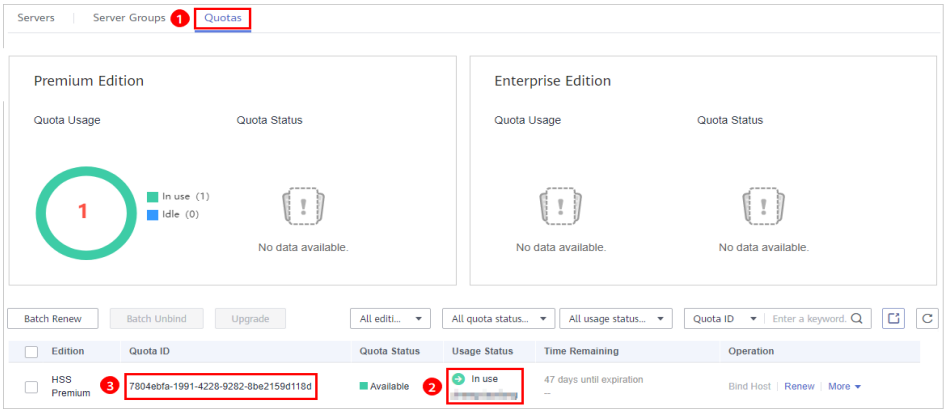

**Step 2** Obtain a quota ID.

- If the **Protection Status** of the server is **Enabled**, click the **Quotas** tab, and find and record its quota ID based on the server name, as shown in **Figure 7-28**.

 Copyright © Huawei Technologies Co., Ltd. 

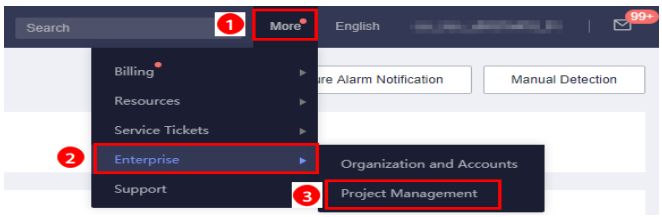
- If the **Protection Status** of the server is **Disabled**, click the **Quotas** tab, and find and record the ID of a quota whose status is **Idle**.

**Figure 7-28** Obtaining a quota ID



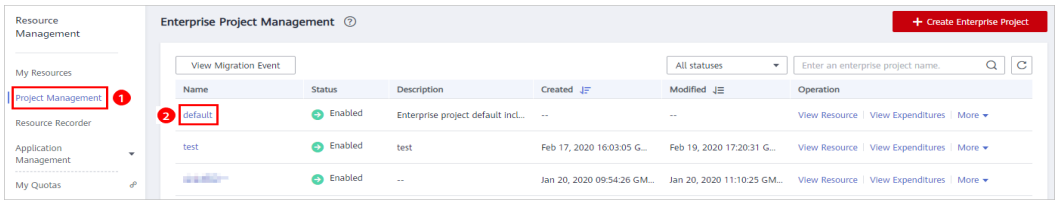

**Step 3** In the upper right corner of the console, choose **Enterprise** > **Project Management**, as shown in **Figure 7-29**.

**Figure 7-29** Choosing Project Management




**Step 4** On the **Project Management** page, click **default** to go to the project details page, as shown in **Figure 7-30**.

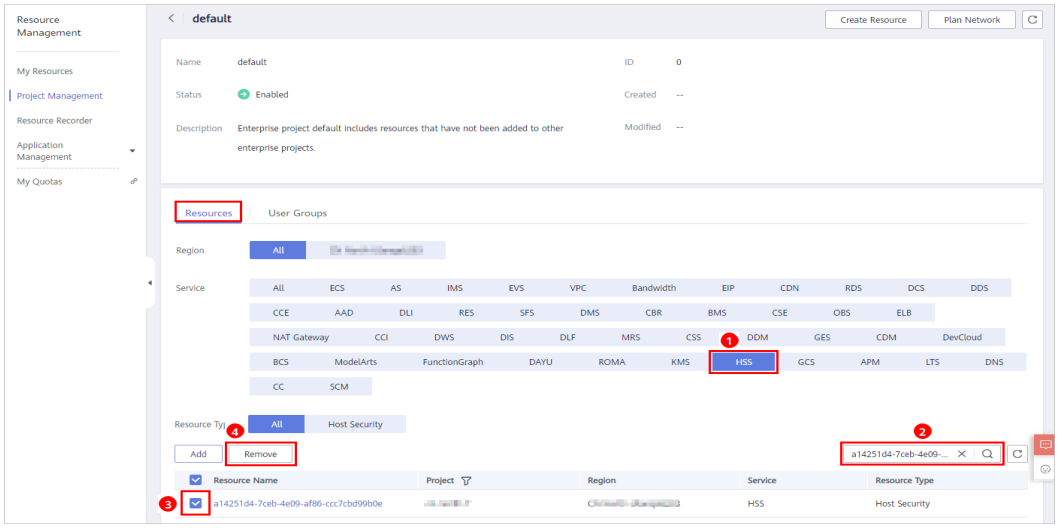
**Figure 7-30** Checking default project details




**Step 5** On the **Resources** tab, select **HSS**, find the quota by the ID obtained in **Step 2**, and remove the quota, as shown in **Figure 7-31**.

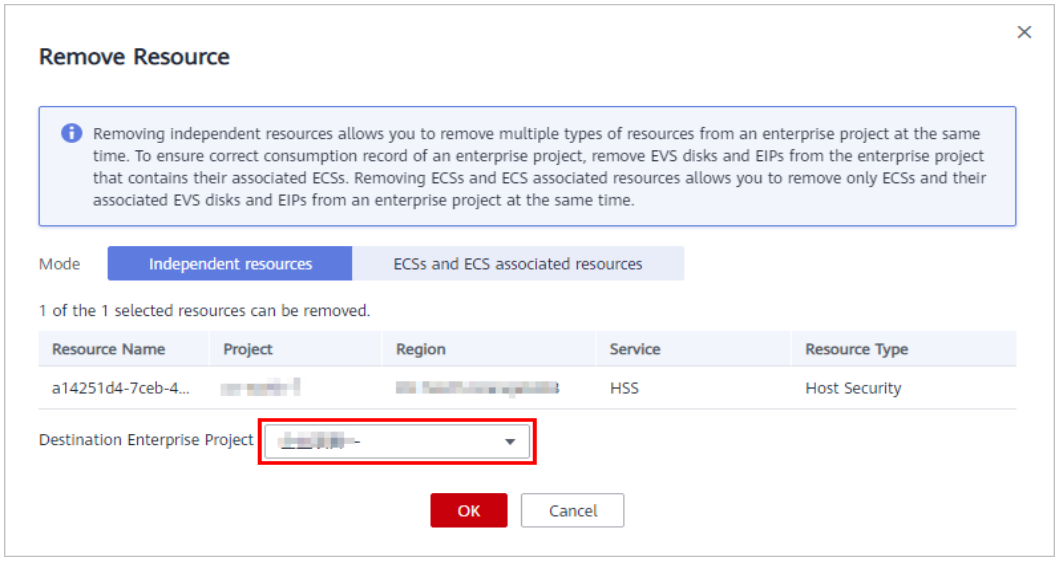
 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-31** Removing the quota




**Step 6** In the displayed **Remove Resource** dialog box, select the project you want to move the resource to, for example, **Enterprise Project 1**, as shown in **Figure 7-32**.

**Figure 7-32** Moving the resource to an enterprise project




**Step 7** Click **OK**. You can use the quota under the enterprise project.

To check the quota, choose **Servers**, select **Enterprise Project 1** from the **Enterprise Project** drop-down list, and click the **Quotas** tab.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

# 8 Fee

## 8.1 Pricing Standards

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

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

## 8.2 If I Do Not Renew HSS After It Expires, Will My Services Be Affected?

HSS is used to improve your server security. Its expiration has no impact on your servers or services.

However, servers not protected by HSS are highly exposed to attacks. Data and programs on the servers will probably be breached or tampered with if the servers are intruded, interrupting your business and causing great loss.

HSS provides all-round protection for servers, including pre-attack prevention, during-attack protection, and real-time or daily alarms. For more information, see **HSS**.

### Follow-Up Procedure

- **Purchase HSS Quota**
- **Renewal**

## 8.3 If I Unsubscribe from HSS and Purchase It Again, Do I Need to Install Agents and Configure Server Protection Settings from Scratch?

If you unsubscribe from HSS, your HSS quota will no longer be available.

HSS neither automatically uninstalls the agent from your servers nor modify or delete the server protection configurations on your servers.

 Copyright © Huawei Technologies Co., Ltd. 

### Old and New HSS Quota Are in the Same Region

You do not need to install the agent or configure server protection again.

### Old and New HSS Quota Are in Different Regions

HSS quotas cannot be used across regions. If you purchased an incorrect quota, unsubscribe from it and purchase a quota in the region of your servers. You do not need to configure server protection again.

## 8.4 How Do I Renew HSS?

You can renew your HSS when it is about to expire. After the renewal, you can continue to use the service.

- Auto-renew

  If you have selected and agreed to auto renewal, the system automatically generates a renewal order and renews the subscription based on the original subscription period before the service expires.

- Manual renewal

  Before the service expires, the system will send an SMS message or email to remind you to renew it.

  If you do not renew the service before it expires, it will enter the retention period.

  The retention period varies with customer tiers. For details, see **Length of Retention Period**.

  In the retention period, HSS will no longer protect your servers, but HSS-related configurations will be retained. When the retention period expires, the HSS-related configurations will be deleted.

  For server security purposes, you are advised to renew your quota in a timely manner.

### Prerequisites

You have obtained the login account (with the **BSS Administrator** and **HSS Administrator** permissions) and password for logging in to the management console.

NOTE

An account with the **BSS Administrator** permission can perform any operation on all menu items in the account center, billing center, and resource center.

### Procedure

**Step 1** **View all quotas** and locate the quota to be renewed.

**Step 2** In the **Operation** column of the quota to be renewed, click **Renew**.

**Step 3** Complete the renewal as prompted on the corresponding page.

 Copyright © Huawei Technologies Co., Ltd. 

For more details, see **Manually Renewing a Resource**.

**----End**

# 8.5 How Do I Apply for Unsubscription and Refund?

- If you purchased HSS in the wrong edition or region, you can first unsubscribe from it and then purchase the correct quota.
- You can unsubscribe from idle quota to save cost.

## Prerequisites

- You have obtained the login account (with the **HSS Administrator** and **BSS Administrator** permissions) and password for logging in to the management console.
- If the quota you want to unsubscribe from is in use, disable its protection on servers and then unsubscribe from it.

## Procedure

**Step 1** **View all quota** and locate the quota to be unsubscribed from.

**Step 2** In the **Operation** column of the quota to be unsubscribed, click **Unsubscribe**.

**Step 3** Complete the unsubscription operations as prompted on the corresponding page.

For details, see **Unsubscription Rules**.

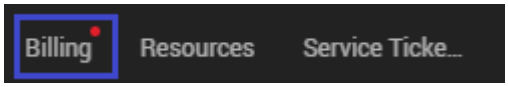
**----End**

## Batch Unsubscription

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

**Step 2** Click **Billing** in the upper right corner of the page.

**Figure 8-1** Entry to the billing center




**Step 3** In the navigation pane, choose **Unsubscriptions and Changes** > **Unsubscriptions**.

**Step 4** Complete the unsubscription operations as prompted on the corresponding page.

For details, see **Unsubscription Rules**.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

# 9 Others

## 9.1 What Are Regions and AZs?

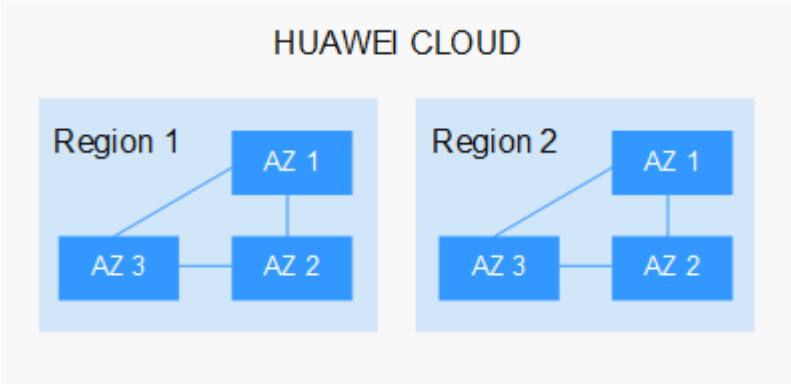
### Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

**Figure 9-1** shows the relationship between the regions and AZs.

**Figure 9-1** Region and AZ




 Copyright © Huawei Technologies Co., Ltd. 

HUAWEI CLOUD provides services in many regions around the world. You can select a region and AZ as needed.

### Selecting a Region

When selecting a region, consider the following factors:

- Location

  You are advised to select a region close to you or your target users. This reduces network latency and improves access rate. However, Chinese mainland regions provide basically the same infrastructure, BGP network quality, as well as operations and configurations on resources. Therefore, if you or your target users are in the Chinese mainland, you do not need to consider the network latency differences when selecting a region.

  - If you or your target users are in the Asia Pacific region, except the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your target users are in Africa, select the **AF-Johannesburg** region.
  - If you or your target users are in Europe, select the **EU-Paris** region.
- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

### Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

### Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

## 9.2 What Should I Do If the Key Board Response Is Slow or If I Need to Enter Consecutive Digits in Chinese Windows OS?

Choose the English input method.

 Copyright © Huawei Technologies Co., Ltd. 

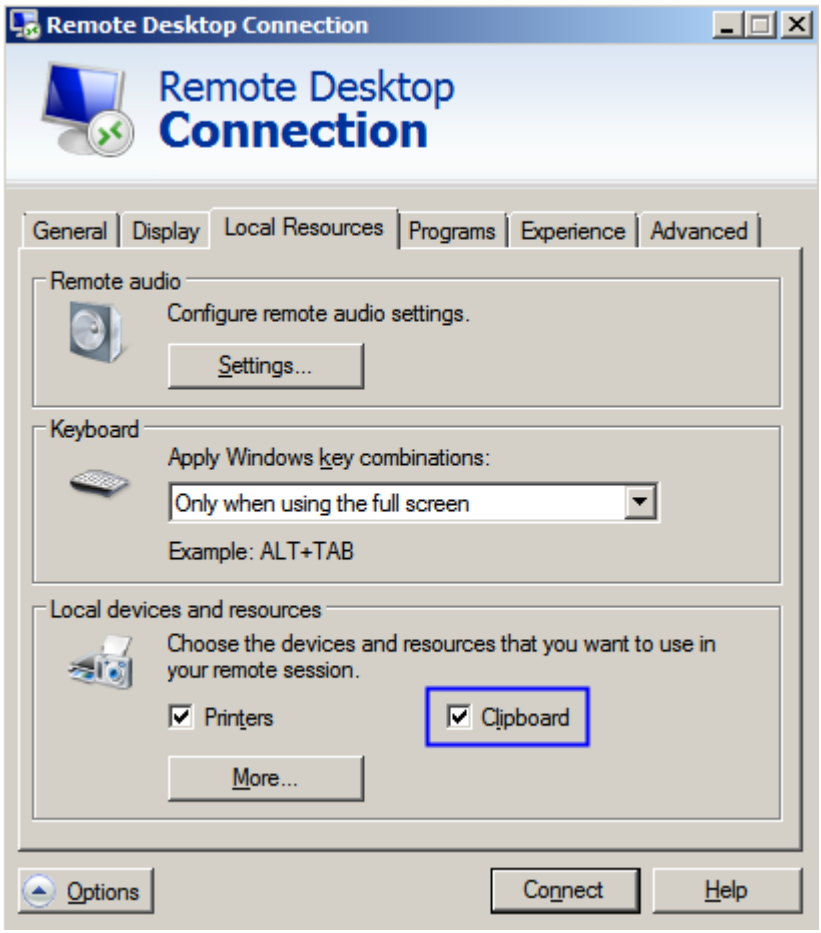
# 9.3 How Do I Use the Windows Remote Desktop Connection Tool to Connect to a Server?

## Procedure

**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**.

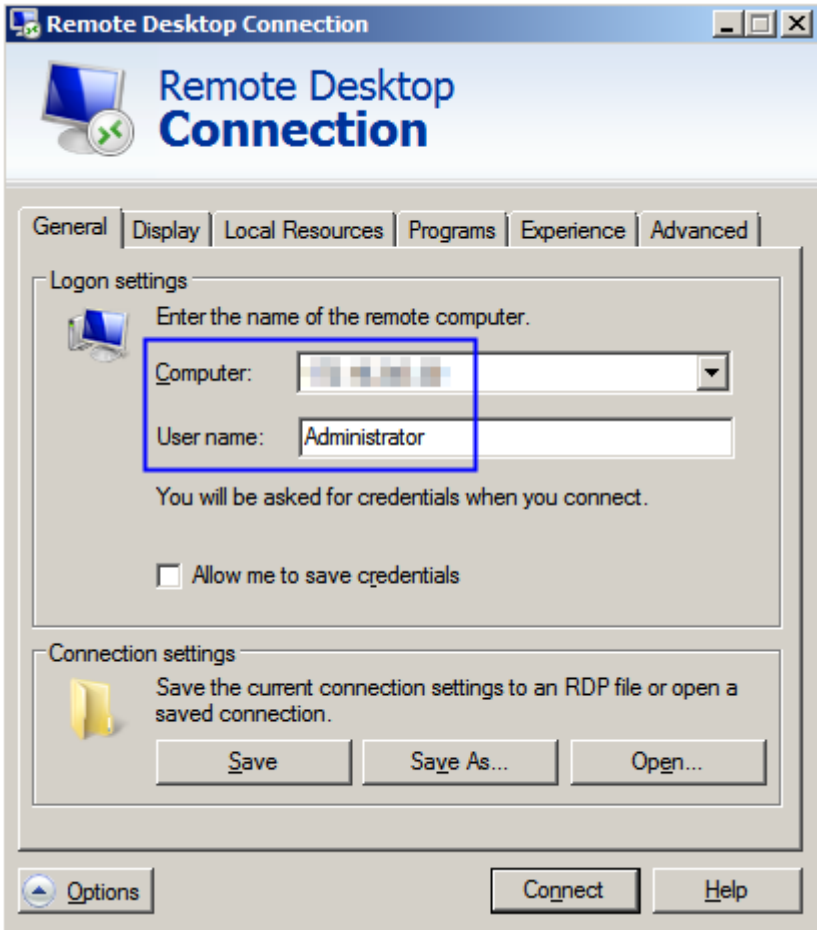
**Figure 9-2** Remote desktop connection




**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**.


Copyright © Huawei Technologies Co., Ltd.

**Figure 9-3** Setting general parameters




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

**----End**

# 9.4 How Do I Check HSS Log Files?

## Log Paths

The following table describes log files and their paths.

| OS | Log Directory | Log File |
| --- | --- | --- |
| Linux | /usr/local/hostguard/log/ | • **daemon.log**: daemon process runtime log<br>• **hostguard.log**: monitoring process runtime log<br>• **hostguard_procmon.log**: process creation log |


Copyright © Huawei Technologies Co., Ltd.

| OS | Log Directory | Log File |
| --- | --- | --- |
| Windows | C:\Program Files (x86)\HostGuard\log\ | • **urlconfig.log**: region log. This is used only during installation.<br>• **daemon.log**: upgrade.log<br>• **hostguard_rsync.log**: run log of the WTP backup server |

### Log Retention

| Log File | Maximum Size | Retained File | Retention Period |
| --- | --- | --- | --- |
| daemon.log | 10 MB | Latest five **daemon.log** files | Until the HSS agent is uninstalled |
| hostguard.log | 10 MB | Latest five **hostguard.log** files | |
| hostguard_procmon.log | 20 MB | Latest two **hostguard_procmon.log** files | |
| urlconfig.log | Unlimited | Only one **urlconfig.log** file | |
| upgrade.log | Unlimited | Only one **upgrade.log** file | |
| hostguard_rsync.log | Unlimited | Only one **hostguard_rsync.log** file | |

# 9.5 How Do I Enable Logging for Login Failures?

## MySQL

The account hacking prevention function for both Windows and Linux OSs 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 Windows OS, modify the **my.ini** file by adding **log_warnings=2** to **[mysqld]**.

 Copyright © Huawei Technologies Co., Ltd. 

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

**----End**

## Filezilla

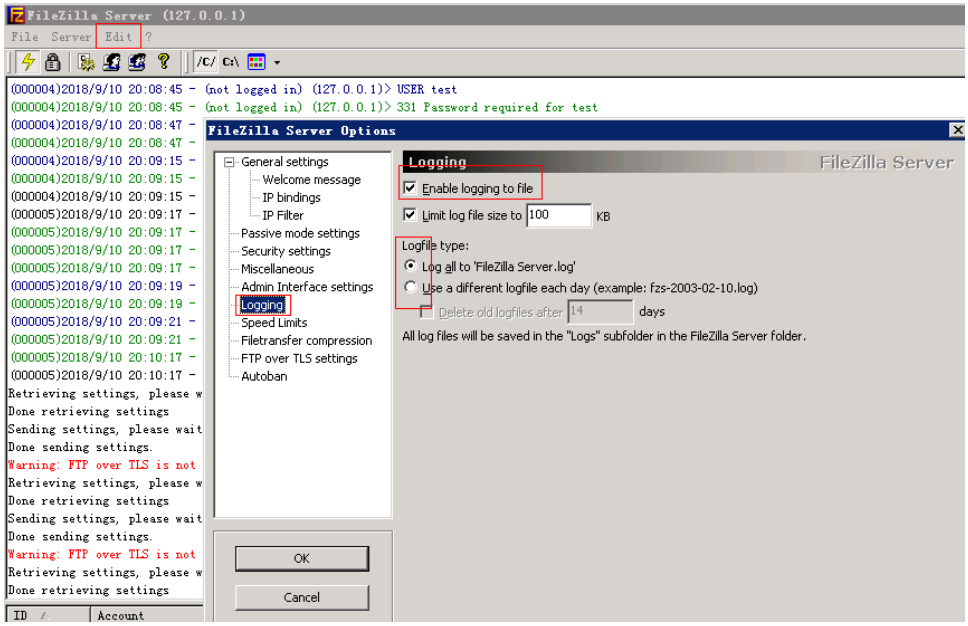
In the account cracking prevention function of HSS, only Windows OSs support FileZilla 0.9.60. Logging is disabled in FileZilla by default.

To enable the logging function, perform the following steps:

**Step 1** Open FileZilla.

**Step 2** Choose **Edit** > **Settings** > **Logging** and select **Enable logging to file** (see **Figure 9-4**).

**Figure 9-4** Enabling logging in FileZilla




**----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:

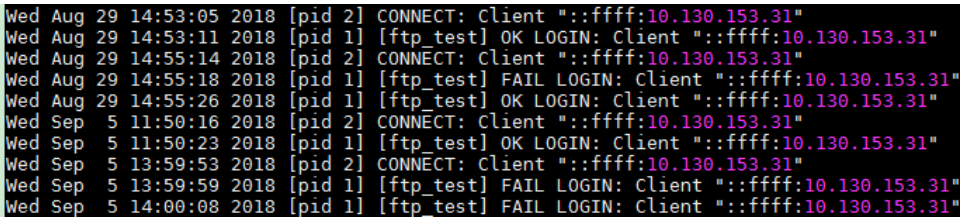
**vsftpd_log_file=log/file/path**

**dual_log_enable=YES**

**Step 2** Restart the vsftp service. If the setting is successful, log records shown in the logs shown in **Figure 9-5** will be returned when you log in to vsftp.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 9-5** Log records




**----End**

# 9.6 How Do I Scan My Servers?

The HSS service detects risks and abnormal operations on servers in real time and performs a comprehensive scan for the servers every early morning. In addition, you can conduct manual detections to check key configuration information on servers.

**NOTICE**

At least a three-minute interval is required between two manual detections for the same item.

## Prerequisites

The **Agent Status** of the server is **Online**, the **Protection Status** is **Enabled**, and the **Edition** is **Enterprise** or **Premium**.

## Check Items

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

## Scan Duration

- The scan for a single item (such as password risks) takes less than 30 minutes.
- A comprehensive manual scan takes less than 30 minutes. Items are scanned concurrently.

## Performing a Manual Scan with One Click

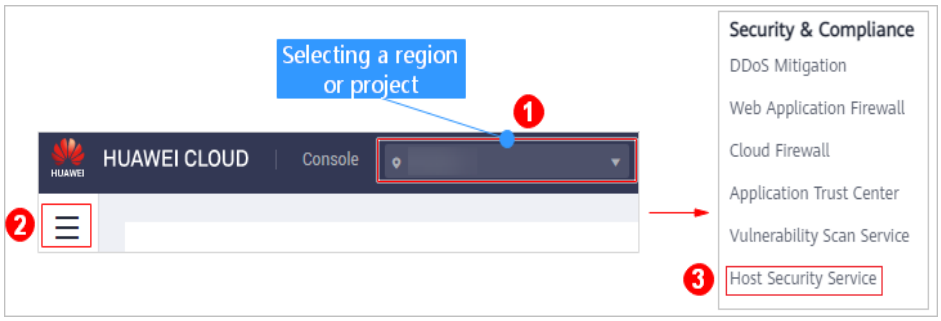
Performing a manual scan with one click can detect risky software information, vulnerabilities, web shells, key configuration information, weak password complexity policies, and accounts using weak passwords on the servers. After the scan is complete, you can view overall risk statistics or the details of a single server on the HSS console.

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

 Copyright © Huawei Technologies Co., Ltd. 

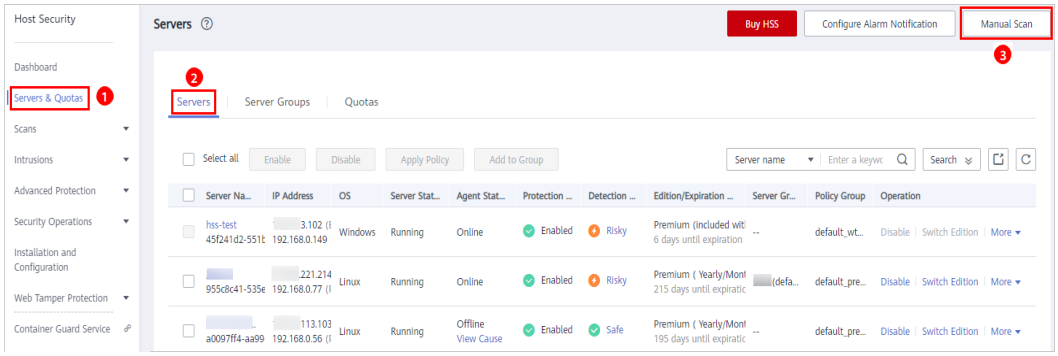
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

**Figure 9-6** Accessing HSS




**Step 3** In the upper right corner of the **Servers** page, click **Manual Scan**.

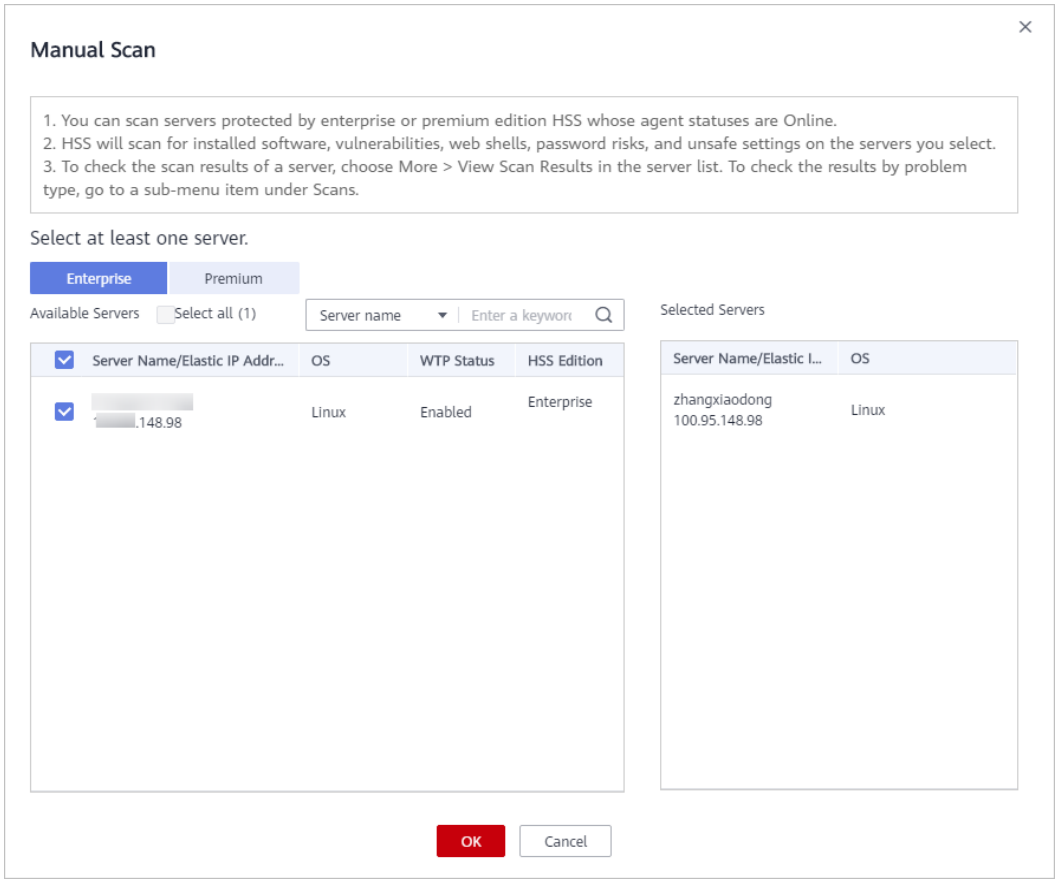
**Figure 9-7** Performing a manual scan




**Step 4** In the **Manual Scan** dialog box, select the target servers and click **OK**.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 9-8** Manual scan




**Step 5** On the **Dashboard** page of the HSS console, view the overall detection result. Alternatively, on the **Servers** page, click **View Scan Results** in the **Operation** column of a server to view the manual detection results of the server.

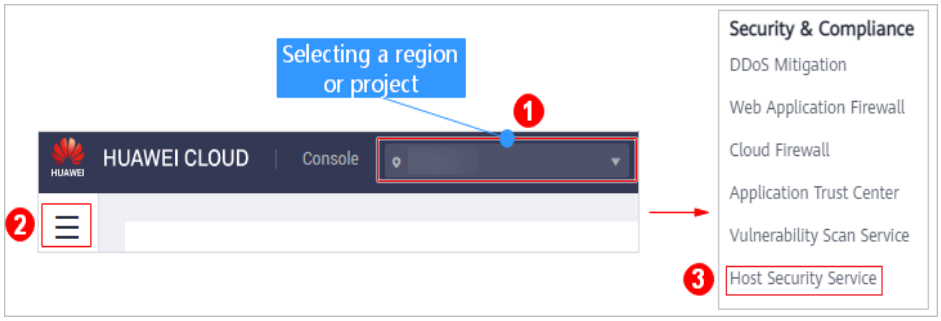
**----End**

## Manually Checking an Item

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

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

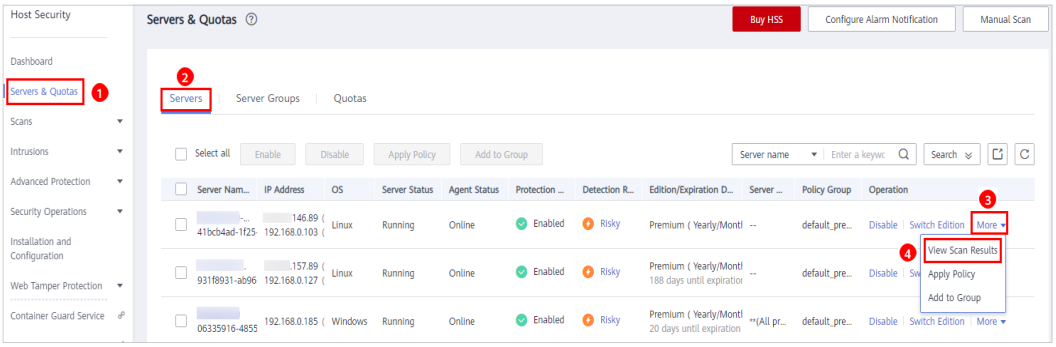
**Figure 9-9** Accessing HSS




 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** In the navigation pane, choose **Servers**. In the **Operation** column of the server list, click **View Scan Results**.

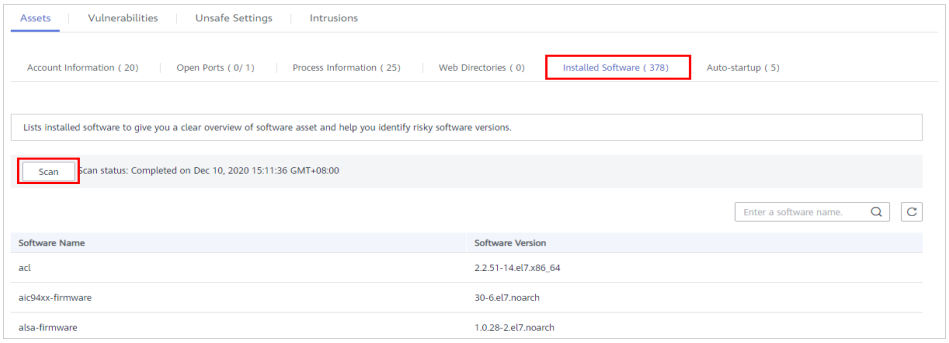
**Figure 9-10** Viewing scan results




- **Checking software information**

  Click **Installed Software** on the **Assets** tab, and click **Scan**.

  **Figure 9-11** Viewing software information




- **Detecting vulnerabilities**

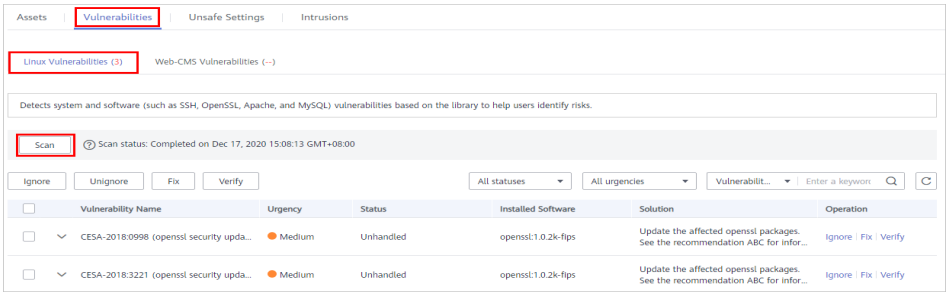
  Click the **Vulnerabilities** tab. Click **Linux Vulnerabilities** or **Web-CMS Vulnerabilities** and click **Scan**.

  NOTE

  The manual detection of either software vulnerabilities or software information management will collect software information from servers.

  – Click Select the **Vulnerability Management** tab, select a system vulnerability, and click **Scan**. HSS will scan for system vulnerabilities immediately.

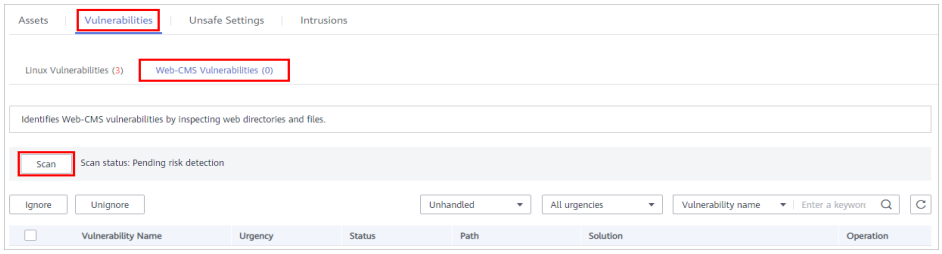
  **Figure 9-12** Detecting system vulnerabilities




 Copyright © Huawei Technologies Co., Ltd. 

– Click the **Vulnerabilities** tab. Click **Web-CMS Vulnerabilities**, select a vulnerability, and click **Scan**. HSS will detect Web-CMS vulnerabilities immediately.

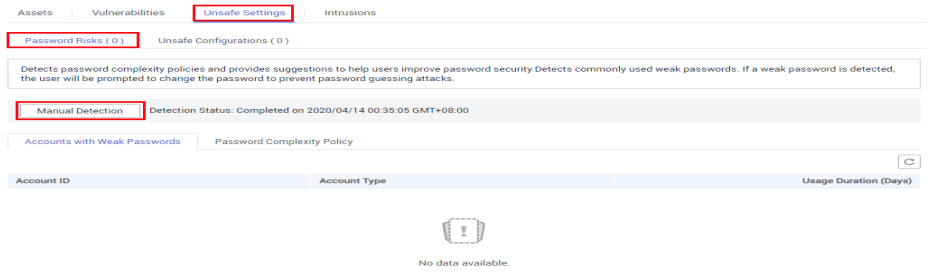
**Figure 9-13** Detecting Web-CMS vulnerabilities




- **Detecting password risks**

  Click the **Unsafe Settings** tab and click **Password Risks**. Click **Scan** to manually detect unsafe configurations.

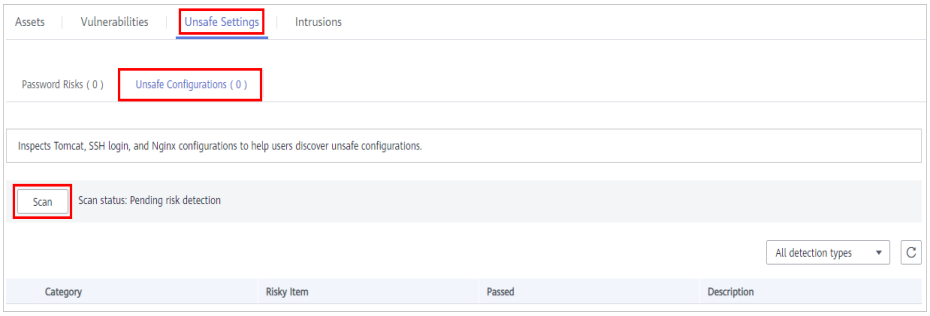
  **Figure 9-14** Detecting weak passwords




- **Detecting unsafe settings**

  Click the **Unsafe Settings** tab and click **Unsafe Configurations**. Click **Scan** to manually detect unsafe configurations.

  **Figure 9-15** Detecting unsafe settings




**Step 4** Wait until **Detection Status** changes to **Completed**, click  to refresh the detection results.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 9.7 Why Does Manual Detection Fail?

Manual detection will probably fail if you perform it too frequently. At least a three-minute interval is required between two manual detections for the same item.

## 9.8 Does HSS Have a Service Level Agreement?

HSS does not have a separate service level agreement (SLA). For details about the general SLA, see **https://www.huaweicloud.com/en-us/declaration/sla.html**.

## 9.9 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.

## 9.10 Is HSS Available as Offline Software?

No.

## 9.11 Do I Have to Bind an EIP to My Server to Install an HSS Agent on the Server?

Yes, because your server must connect to the Internet to download the agent installation package.

However, if you installed the agent on a HUAWEI CLOUD server, you can unbind the EIP from the server after the installation is complete.

## 9.12 Can I Use HSS Via APIs?

Yes. You can use APIs to query ECS statuses and intrusion events in **CN North-Beijing1**, **CN North-Beijing4**, **CN East-Shanghai1**, **CN East-Shanghai2**, **CN South-Guangzhou**, and **CN Southwest-Guiyang1** regions. More open APIs will be available in more regions soon.

## 9.13 Can HSS Alarm Logs Be Stored in OBS?

No. The log files are stored in the service folder. For details about the storage path and log retention period, see **How Do I Check HSS Log Files?**


Copyright © Huawei Technologies Co., Ltd.

# 9.14 How Do I Change the Server Bound to an HSS Quota?

Unbind the quota from the existing server and bind it to a new server. The procedure is as follows:

1. Unbind the quota from the existing server. For details, see **Unbinding a Quota from a Server**.
2. Bind the quota to a new server. For detail, see **Binding a Quota to a Server**.
3. **Check the quota status**.

NOTE

To enhance server security, you can **ugrade a quota**.


Copyright © Huawei Technologies Co., Ltd.

# A Change History

| Released On | Description |
| --- | --- |
| 2022-01-29 | This is the thirty-eighth official release.<br>Added the following FAQs:<br>**How Do I Enable the HSS Basic Edition Free of Charge?**<br>**How Does HSS Transfer Data?** |
| 2022-01-13 | This is the thirty-seventh official release.<br>Improved the following sections:<br>**How Do I Defend Against Brute-force Attacks?**<br>**How Do I Handle Alarms on the Brute-Force Attacks Launched from a HUAWEI CLOUD IP Address?** |
| 2021-10-22 | This is the thirty-sixth official release.<br>Added the following FAQs:<br>**How Do I Handle Alarms on the Brute-Force Attacks Launched from a HUAWEI CLOUD IP Address?**<br>**Can I Check the Vulnerability and Baseline Fix History on HSS?** |

 Copyright © Huawei Technologies Co., Ltd. 

| Released On | Description |
| --- | --- |
| 2021-10-18 | This is the thirty-fifth official release.<br>Added the following FAQs:<br>• **How Do I Change the Server Bound to an HSS Quota?**<br>• **How Often Does HSS Detect, Isolate, and Kill Malicious Programs?**<br>• **How Often Are the HSS Virus Database and Vulnerability Database Updated?**<br>• **Do I Have to Deploy HSS on All My Cloud Servers?**<br>• **What Do I Do If HSS Frequently Reports Brute-force Alarms?**<br>• **How Do I Check Vulnerability Severity?**<br>Modified the following FAQ:<br>• **What Do I Do If Agent Installation Fails?** |
| 2021-08-03 | This is the thirty-fourth official release.<br>Added the following FAQ:<br>• **Do I Need to Enable HSS Again After My Server OS Is Reinstalled?**<br>Modified the following FAQs:<br>• **How Do I Fix an Abnormal Agent?**<br>• **How Do I Purchase and Enable HSS?** |
| 2021-07-14 | This is the thirty-third official release.<br>Added the following FAQs:<br>• **How Do I Modify Alarm Notification Items?**<br>• **If I Change the OS of a Protected Server, Does It Affect My HSS Quota?**<br>• **How Do I Filter Unprotected Servers?**<br>• **Can I Add an IP Blacklist in HSS?**<br>• **What Are the Differences Between HSS and SA Baseline Checks?**<br>• **How Do I Purchase and Enable HSS?**<br>Modified the following FAQs:<br>• **What Do I Do If Agent Installation Fails?**<br>• **What Do I Do If an Alarm Still Exists After I Fixed a Vulnerability?** |
| 2021-07-08 | This is the thirty-second official release.<br>Added the links for uninstalling and installing the agent in **How Do I Fix an Abnormal Agent?**. |


Copyright © Huawei Technologies Co., Ltd.

| Released On | Description |
| --- | --- |
| 2021-06-08 | This is the thirty-first official release.<br>Added the following FAQs:<br>• **Does HSS Agent Installation Affect My Services?**<br>• **How Do I Unblock an IP Address?**<br>• What Do I Do If an Alarm Still Exists After I Fixed a Kernel Vulnerability?<br>• **What Do I Do If an Alarm Still Exists After I Fixed a Vulnerability?**<br>• **Can HSS Alarm Logs Be Stored in OBS?**<br>Modified the following FAQs:<br>• **How Does HSS Block Brute-Force Attacks?**<br>• **How Do I Handle a Brute-force Attack Alarm?**<br>• **How Do I Defend Against Brute-force Attacks?**<br>• **Do I Need to Restart a Server After Fixing its Vulnerabilities?** |
| 2021-04-28 | This is the thirtieth official release.<br>• Added the following FAQs:<br>– **How Do I Install the Agent from the Command Line (on Windows)?**<br>– **Why Are the Weak Password Alarms Still Reported After the Weak Password Policy Is Disabled?**<br>• Modified the following FAQs:<br>– **How Do I Fix an Abnormal Agent?**<br>– **Why Do I Still Receive Remote Login Alarms After Configuring the Login IP Whitelist?** |
| 2021-02-25 | This is the twenty-ninth official release.<br>Modified description in **Can I Disable HSS Alarm Notifications?** You can enable HSS without enabling alarm notifications. |
| 2021-02-01 | This is the twenty-eighth official release.<br>Added the following FAQs:<br>• **Can HSS Protect Offline Servers Using the Same Public IP Address?**<br>• **Can I Bind a Server to an HSS Quota If They Are in Different Enterprise Projects?**<br>• **Why Can't I Select Free HSS When Purchasing ECS?** |
| 2020-11-16 | This is the twenty-seventh official release.<br>Cross-region usage is not supported in **Can HSS Quota Be Shared Across Regions?**. |


Copyright © Huawei Technologies Co., Ltd.

| Released On | Description |
| --- | --- |
| 2020-11-10 | This is the twenty-sixth official release.<br>Added the following FAQs:<br>• **How Do I Handle a Brute-force Attack Alarm?**<br>• **How Do I Handle a Weak Password Alarm?**<br>• **What Do I Do If My Servers Are Subjected to a Mining Attack?**<br>• **Why a Process Is Still Isolated After It Was Whitelisted?**<br>• **Why Do I Still Receive Remote Login Alarms After Configuring the Login IP Whitelist?**<br>• **How Do I Modify Alarm Notification Recipients?** |
| 2020-06-20 | This is the twenty-fifth official release.<br>Added **How Do I Migrate Settings Between Projects After Enabling Enterprise Projects for HSS?**. |
| 2020-05-18 | This is the twenty-fourth official release.<br>Added the following FAQs:<br>• **What Are the Differences Between the Web Tamper Protection Functions of HSS and WAF?**<br>• **How Do I Check HSS Log Files?** |
| 2020-03-09 | This issue is the twenty-third official release.<br>Added the following FAQs:<br>• **How Do I Filter Servers Where No Agents Have Been Installed?**<br>• **Why Does My Login Fail After I Enable 2FA?**<br>• **How Do I Configure My Mobile Number When Enabling 2FA?**<br>• **If I Choose to Use Verification Code for 2FA, How Do I Get the Code?**<br>• **What Can I Do If I Enabled Dynamic WTP But Its Status Is Enabled but not in effect?**<br>• **How Do I Clear the SSH Login IP Address Whitelist Configured in HSS?** |
| 2020-01-14 | This is the twenty-second official release.<br>Added the following FAQs:<br>• **What Is the HSS Agent?**<br>• **Can I Disable HSS Alarm Notification?** |


Copyright © Huawei Technologies Co., Ltd.

| Released On | Description |
| --- | --- |
| 2019-12-26 | This is the twenty-first official release.<br>Added the following FAQs:<br>• **Can HSS Quota Be Shared Between Accounts?**<br>• **Do I Need to Install the HSS Agent After Purchasing HSS?** |
| 2019-12-18 | This is the twentieth official release.<br>Deleted the following FAQs:<br>Can I Subscribe to a Weekly Report of HUAWEI CLOUD HSS? |
| 2019-11-27 | This is the nineteenth official release.<br>Added the following FAQs:<br>• **If I Do Not Renew HSS After It Expires, Will My Services Be Affected?**<br>• **How Do I Modify a File After WTP Is Enabled?**<br>• **Why No Topics Are Available for Me to Choose When I Configure Alarm Notifications?**<br>• **How Do I Prevent Account Cracking Attacks?**<br>• **Why a Message Indicating Insufficient Quota Is Displayed When I Enable Protection?** |
| 2019-10-12 | This is the eighteenth official release.<br>Added the following FAQs:<br>**How Do I Fix Vulnerabilities?** |
| 2019-09-23 | This issue is the seventeenth official release.<br>Added the following FAQs:<br>• **Can I Upgrade the Basic Edition HSS to the Enterprise Edition?**<br>• **Why a Blocked IP Address Is Automatically Unblocked?**<br>• How Do I Handle Configuration Risks Detected in a Baseline Check?<br>• **Why Do I Need to Add a Protected Directory?**<br>• **What Should I Do If WTP Cannot Be Enabled?** |
| 2019-04-25 | This is the thirteenth official release.<br>Added the following FAQs:<br>Can I Upgrade the Enterprise Edition to the WTP Edition? |
| 2019-04-08 | This issue is the sixteenth official release.<br>Updated the screenshots and related descriptions in section **How Do I Use 2FA?** |


Copyright © Huawei Technologies Co., Ltd.

| Released On | Description |
| --- | --- |
| 2019-03-18 | This issue is the fifteenth official release.<br>Added the following FAQs:<br>Does HSS Protect Bare Metal Servers? |
| 2018-11-06 | This is the fourteenth official release.<br>Added the following FAQs:<br>• **What Should I Do If the Key Board Response Is Slow or If I Need to Enter Consecutive Digits in Chinese Windows OS?**<br>• **How Do I Install the Agent on Servers in Batches?** |
| 2018-10-25 | This is the thirteenth official release.<br>Added the following FAQs:<br>**How Do I Install the Agent on Servers in Batches?** |
| 2018-09-15 | This is the twelfth official release.<br>Added the following FAQs:<br>• **How Do I Enable Logging for Login Failures?**<br>• How Do I Enable Logging for Failure of Login to FileZilla?<br>• How Do I Enable Logging for Failure of Login to vsftp? |
| 2018-08-02 | This is the eleventh official release.<br>Added the following FAQs:<br>**What Should I Do If the Account Cracking Prevention Function Does Not Take Effect on Some Accounts in Linux OSs?** |
| 2018-07-19 | This is the tenth official release.<br>Added the following FAQs:<br>What Should I Do When My Settings of IP Address Interception for Account Cracking Prevention Fail in SUSE12 SP2 and Gentoo Systems? |
| 2018-06-28 | This is the ninth official release.<br>Added the following FAQs:<br>How Do I Set a Secure Password Complexity Policy in a Windows OS? |
| 2018-06-13 | This is the eighth official release.<br>Added the following FAQs:<br>How Do I Install the Agent on Servers in Batches? |
| 2018-05-17 | This is the seventh official release.<br>Optimized FAQ titles. |


Copyright © Huawei Technologies Co., Ltd.

| Released On | Description |
| --- | --- |
| 2018-05-07 | This is the sixth official release.<br>Added the following FAQs:<br>Does HSS Charge Fees? |
| 2018-04-19 | This is the fifth official release.<br>Added the following FAQs:<br>Updated the screenshots in "How Do I Install an HSS Agent?" |
| 2018-03-15 | This is the fourth official release.<br>Deleted the following FAQs:<br>What Should I Do When an Error Is Displayed When I Install an Agent in a Windows OS? |
| 2018-01-09 | This is the third official release.<br>Added the following FAQs:<br>How Do I Install the Agent? |
| 2017-11-17 | This is the second official release.<br>Added the following FAQs:<br>How Do I Install a PAM and Set a Proper Password Complexity Policy? |
| 2017-09-30 | This is the first official release. |


Copyright © Huawei Technologies Co., Ltd.