Host Security Service (HSS)

Best Practices

Issue 03
Date 2024-03-12

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
              Bantian, Longgang
              Shenzhen 518129
              People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Best Practices of Login Security Hardening

Account and password cracking are the most commonly used ways for attackers to intrude or attack servers. Enhancing login security is the first step to protect server security and ensure that services can run properly.

Prerequisites

You have purchased an ECS and enabled protection for it.

Login Security Hardening Functions

You can configure common login locations, common login IP addresses, SSH login IP address whitelist, two-factor authentication, weak password check, and login security check to protect login security.

To ensure high login security, you are advised to configure all of these functions.

□ **NOTE**

Two-factor login authentication is supported by the HSS basic edition billed in yearly/monthly mode, by the enterprise or higher edition. Login security check is supported by the HSS enterprise edition or higher. Other protection functions are available in the HSS basic edition.

Figure 1-1 HSS login security hardening functions
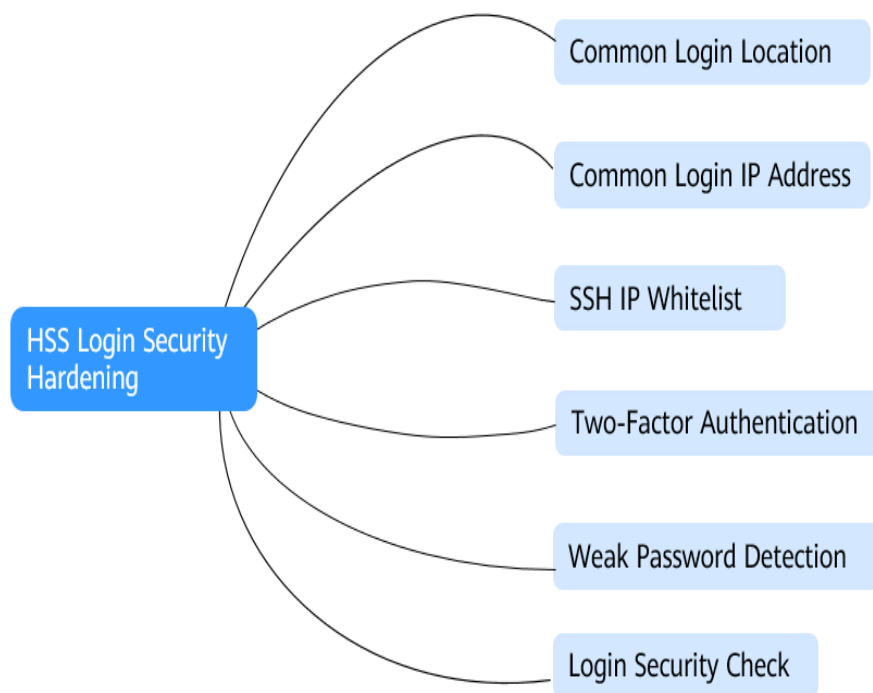
Configuring Common Login Locations

After common login locations are configured, Host Security Service will generate alarms for logins to ECSs in non-common login locations. You can add multiple common login locations for each ECS.

Constraints

An account can add up to 10 common login locations.

Procedure

Step 1 Choose **Installation & Configuration** and click the **Security Configuration** tab. Click **Common Login Locations** and click **Add Common Login Location**.

Figure 1-2 Adding a common login location
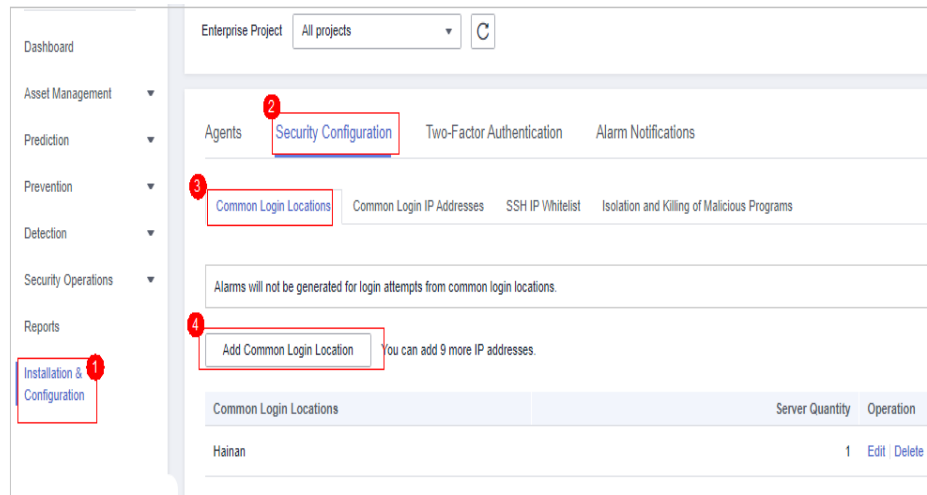
Step 2 In the dialog box that is displayed, select a geographical location and select servers. Confirm the information and click **OK**.

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

----End

Configuring Common Login IP Address

After you configure common login IP addresses, Host Security Service will generate alarms on the logins from other login IP addresses.

Constraint

An account can add up to 20 common login IP addresses.

Procedure

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

Figure 1-3 Adding a common login IP address

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

> 📖 **NOTE**
>
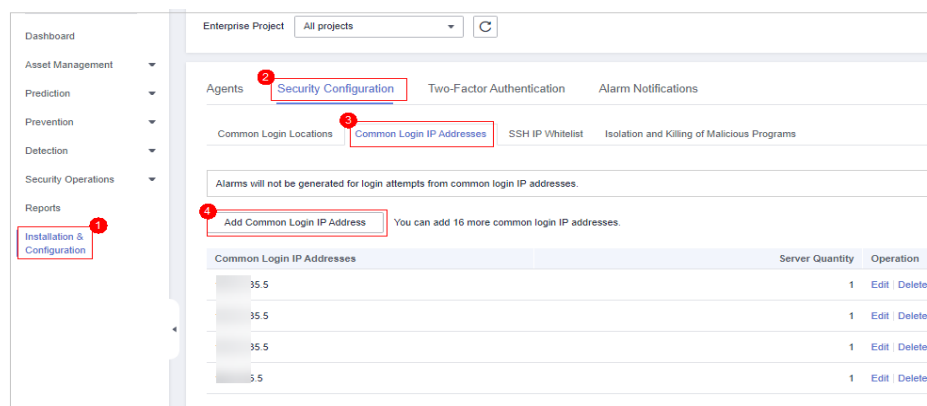> - A common login IP address must be a public IP address or IP address segment.
> - Only one IP address can be added at a time. To add multiple IP addresses, repeat the operations until all IP addresses are added.

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

----End

Configuring SSH Login IP Address Whitelist

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

> 📖 **NOTE**
>
> - An account can have up to 10 SSH login IP addresses in the whitelist.
> - The SSH IP address whitelist does not take effect for servers running Kunpeng EulerOS (EulerOS with Arm).
> - After you configure an SSH login IP address whitelist, SSH logins will be allowed only from whitelisted IP addresses.
>   - Before enabling this function, ensure that all IP addresses that need to initiate SSH logins are added to the whitelist. Otherwise, you cannot remotely log in to your server using SSH.
>
>   If your service needs to access a server, but not necessarily via SSH, you do not need to add its IP address to the whitelist.
>   - Exercise caution when adding an IP address to the whitelist. This will make HSS no longer restrict access from this IP address to your servers.

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

Figure 1-4 Configuring an IP address whitelist
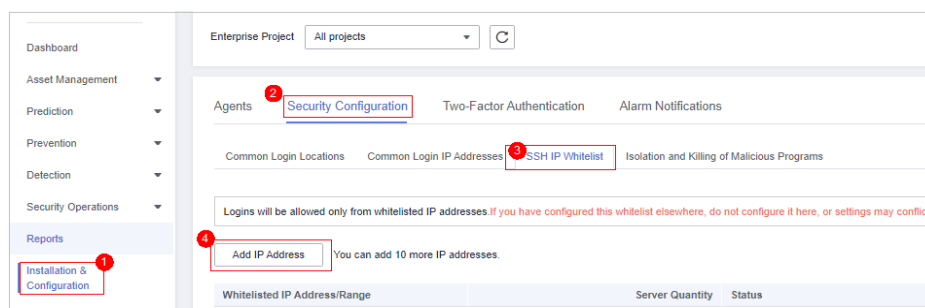
Step 2 In the dialog box that is displayed, enter an IP address and select servers. Confirm the information and click **OK**.

📖 **NOTE**

- A common login IP address must be a public IP address or IP address segment.
- Only one IP address can be added at a time. To add multiple IP addresses, repeat the operations until all IP addresses are added.

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

----End

Configuring Two-Factor Authentication

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

You have to choose an SMN topic for servers where 2FA is enabled. The topic specifies the recipients of login verification codes, and Host Security Service will authenticate login users accordingly.

Prerequisites

- You have created a message topic whose protocol is SMS or email.
- Server protection has been enabled.
- Linux servers require user passwords for login.
- On a Windows server, 2FA may conflict with G01 and 360 Guard (server edition). You are advised to stop them.

Constraints

- If 2FA is enabled, you cannot log in to the servers running a GUI Linux.
- If you have enabled 2FA on a Linux server, you cannot log in to it through CBH.
- 2FA is supported only when the OpenSSH version of Linux is earlier than 8.

Procedure

Step 1 Choose **Installation & Configuration** > **Two-Factor Authentication**.

- Locate the target server and click **Enable 2FA** in the **Operation** column.
- Select multiple target servers and click **Enable 2FA** to enable two-factor authentication for multiple servers in batches.

Step 2 In the displayed dialog box, select a verification mode.

- **SMS/Email**

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

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

- **Verification code**

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

Step 3 Click **OK**.

Step 4 Return to the **Two-Factor Authentication** tab of the **Installation & Configuration** page. Check whether the **2FA Status** of the target server changes to **Enabled**.

It takes about 5 minutes for the two-factor authentication function to take effect.

> **NOTICE**
>
> When you log in to a remote Windows server from another Windows server where 2FA is enabled, you need to manually add credentials on the latter. Otherwise, the login will fail.
>
> To add credentials, choose **Start** > **Control Panel**, and click **User Accounts**. Click **Manage your credentials** and then click **Add a Windows credential**. Add the username and password of the remote server that you want to access.

----End

Configuring Weak Password Detection

Weak passwords are not attributed to a certain type of vulnerabilities, but they bring no less security risks than any type of vulnerabilities.

Data and programs will become insecure if their passwords are cracked.

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

Step 1 Choose **Security Operation** > **Policies**.

Figure 1-5 Accessing the policy group page
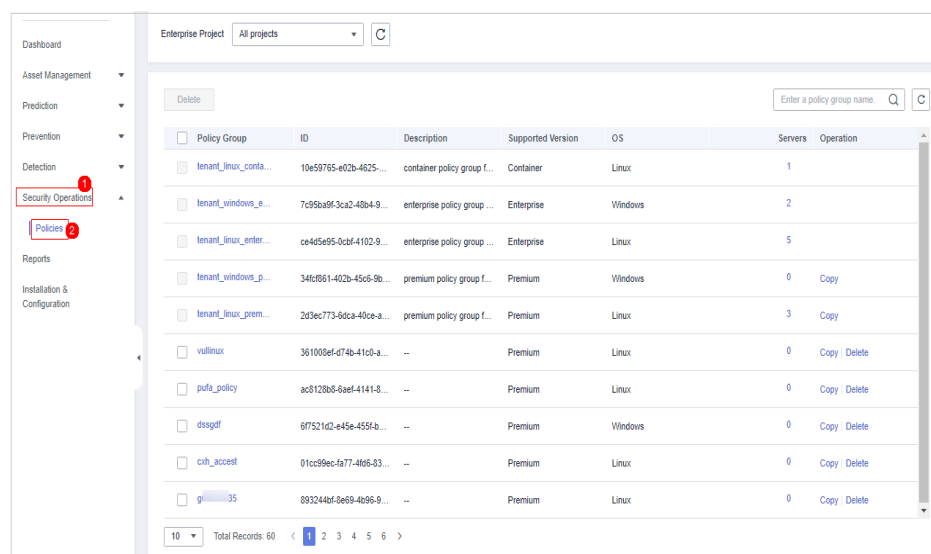
Step 2 Click the name of the target policy group. The policy group page is displayed.

You can determine the OS and protection version supported by the target policy based on its default **Policy Group Name** and **Supported Version**.

📖 **NOTE**

> If you need to create a policy group, perform this step after **Creating a Policy Group**.

Step 3 In the policy group list, click the **Weak password detection**.

Step 4 The **Weak Password Detection** dialog box is displayed. You can modify the parameters in the **Policy Settings** area or retain the default values (recommended). For details about the parameters, see **Table 1-1**.

Table 1-1 Parameter description

Parameter	Description
Scan Time	Time point when detections are performed. It can be accurate to the minute.
Random Deviation Time (s)	Random deviation time of the weak password based on **Scan Time**. The value range is 0 to 7200s.
Scan Days	Days in a week when weak passwords are scanned. You can select one or more days.
User-defined Weak Passwords	You can add a password that may have been leaked to this weak password text box to prevent server accounts from using the password. Enter only one weak password per line. Up to 300 weak passwords can be added.

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

Step 6 Choose **Asset Management** > **Servers & Quota**, click **Servers**, select the target servers, and click **Apply Policy** above the server list.

📖 **NOTE**

> If you need to deploy the same policy for multiple servers at the same time, ensure that the **OS** and **Edition** of the selected servers are the same as those of the target policy.

Step 7 In the policy deployment dialog box, select the target policy group and click **OK**.

Step 8 After the deployment is complete, choose **Security Operations** > **Policies**. Locate the target policy, click the value in the **Servers** column, and check whether the servers you added are displayed.

📖 **NOTE**

> After the deployment is complete, wait for about 1 minute and then check whether the deployment is successful.

**----End**

Configuring Login Security Check

After login security is configured, you can enable login security check for the target server. HSS will effectively detect brute force attacks, automatically block brute force IP addresses, and trigger and report alarms.

📖 **NOTE**

Only the enterprise edition and later support login security check. For enterprise edition, the login security check is performed based on the default parameters and custom parameter configuration is not supported.

Step 1 Choose **Security Operation** > **Policies**.

Figure 1-6 Accessing the policy group page
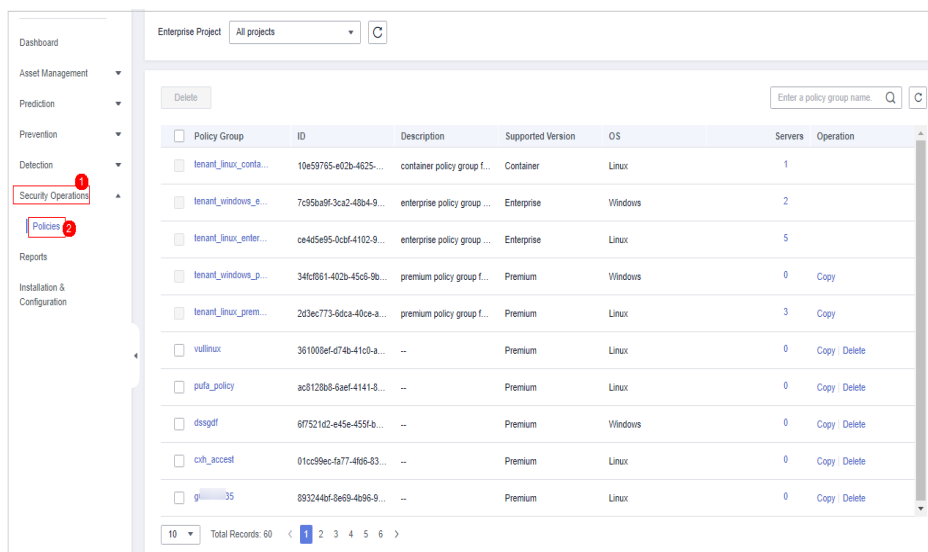
Step 2 Click the name of the target policy group. The policy group page is displayed.

You can determine the OS and protection version supported by the target policy based on its default **Policy Group Name** and **Supported Version**.

📖 **NOTE**

If you need to create a policy group, perform this step after **Creating a Policy Group**.

Step 3 Click **Login Security Check** from the policy list.

Step 4 The **Login Security Check** dialog box is displayed. You can modify the parameters in the **Policy Settings** area or retain the default values. For details about the parameters, see **Table 1-2**.

Table 1-2 Parameter description

Parameter	Description
Lock Time (min)	This parameter is used to determine how many minutes the IP addresses that send attacks are locked. The value range is 1 to 43200. Login is not allowed in the lockout duration.

Parameter	Description
Cracking Behavior Determination Threshold (s)	This parameter is used together with **Cracking Behavior Determination Threshold (Login Attempts)**. The value range is 5 to 3,600. For example, if this parameter is set to **30** and **Cracking Behavior Determination Threshold (Login Attempts)** is set to **5**, the system determines that an account is cracked when the same IP address fails to log in to the system for five times within 30 seconds.
Cracking Behavior Determination Threshold (Login Attempts)	This parameter is used together with **Cracking Behavior Determination Threshold**. The value range is 1 to 36,000.
Threshold for slow brute force attack (second)	This parameter is used together with **Threshold for slow brute force attack (failed login attempt)**. The value range is 600 to 86,400s. For example, if this parameter is set to **3600** and **Threshold for slow brute force attack (failed login attempt)** is set to **15**, the system determines that an account is cracked when the same IP address fails to log in to the system for fifteen times within 3,600 seconds.
Threshold for slow brute-force attack (failed login attempt)	This parameter is used together with **Threshold for slow brute force attack (second)**. The value range is 6 to 100.

Check Whether the Audit Login Is Successful	● After this function is enabled, HSS reports login success logs.
	
	  – ⬤ : enabled
	  – ◯ : disabled

Block Non-whitelisted Attack IP Address	After this function is enabled, HSS blocks the login of brute force IP addresses (non-whitelisted IP addresses).

Report Alarm on Brute-force Attack from Whitelisted IP Address	● After this function is enabled, HSS generates alarms for brute force attacks from whitelisted IP addresses.
	
	  – ⬤ : enabled
	  – ◯ : disabled

Whitelist	After an IP address is added to the whitelist, HSS does not block brute force attacks from the IP address in the whitelist. A maximum of 50 IP addresses or network segments can be added to the whitelist. Both IPv4 and IPv6 addresses are supported.

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

Step 6 Choose **Asset Management** > **Servers & Quota**, click **Servers**, select the target servers, and click **Apply Policy** above the server list.

> **NOTE**
>
> If you need to deploy the same policy for multiple servers at the same time, ensure that the **OS** and **Edition** of the selected servers are the same as those of the target policy.

Step 7 In the policy deployment dialog box, select the target policy group and click **OK**.

Step 8 After the deployment is complete, choose **Security Operations** > **Policies**. Locate the target policy, click the value in the **Servers** column, and check whether the servers you added are displayed.

> **NOTE**
>
> After the deployment is complete, wait for about 1 minute and then check whether the deployment is successful.

----End

2 Detecting and Fixing Vulnerabilities

2.1 Git Credential Disclosure Vulnerability (CVE-2020-5260)

Git issued a security bulletin announcing a vulnerability that could reveal Git user credentials (CVE-2020-5260). Git uses a credential helper to store and retrieve credentials.

But when a URL contains an encoded newline (%0a), it may inject unexpected values into the protocol stream of the credential helper. This vulnerability is triggered when the affected version of Git is used to execute a git clone command on a malicious URL.

Vulnerability ID

CVE-2020-5260

Vulnerability Name

Git credential disclosure vulnerability

Scope of Impact

Affected versions:

- Git 2.17.x <= 2.17.3
- Git 2.18.x <= 2.18.2
- Git 2.19.x <= 2.19.3
- Git 2.20.x <= 2.20.2
- Git 2.21.x <= 2.21.1
- Git 2.22.x <= 2.22.2
- Git 2.23.x <= 2.23.1
- Git 2.24.x <= 2.24.1

- Git 2.25.x <= 2.25.2
- Git 2.26.x <= 2.26.0

Unaffected versions:

- Git 2.17.4
- Git 2.18.3
- Git 2.19.4
- Git 2.20.3
- Git 2.21.2
- Git 2.22.3
- Git 2.23.2
- Git 2.24.2
- Git 2.25.3
- Git 2.26.1

Official Solution

This vulnerability has been fixed in the latest official version. If your service version falls into the affected range, upgrade it to the latest secure version.
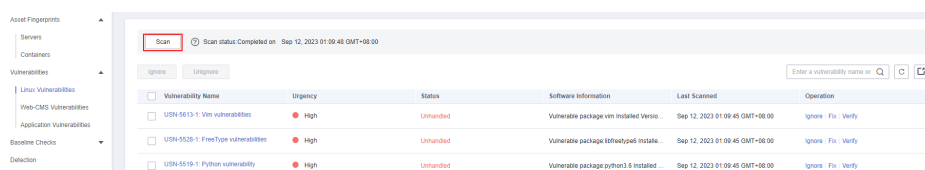
Download address: **https://github.com/git/git/releases**

Suggestion

Perform the following steps to scan and fix a vulnerability.

Step 1 Detect and view vulnerability details, as shown in **Manually starting a vulnerability scan**. For details, see **Viewing Vulnerability Details**.

Figure 2-1 Manually starting a vulnerability scan

Step 2 Fix vulnerabilities and verify the result. For details, see **Handling Vulnerabilities**..

----End

Other Protection Measures

If you cannot perform upgrade for the moment, you can take the following measures:

- Disable credential helper by running the following commands:

  git config --unset credential.helper

  git config --global --unset credential.helper

  git config --system --unset credential.helper

- Be vigilant about malicious URLs.

  a. Examine the server name and username portion of URLs fed to **git clone** for the presence of encoded newlines (%0a) or evidence of credential-protocol injections (example: **host=github.com**).

  b. Avoid using submodules with untrusted repositories (do not use **clone – recurse-submodules**; use **git submodule update** only after examining the URLs found in gitmodules).

  c. Avoid tools which may run git clone.

2.2 SaltStack Remote Command Execution Vulnerabilities (CVE-2020-11651 and CVE-2020-11652)

Security researchers discovered two serious vulnerabilities in SaltStack's products. SaltStack provides a set of product offerings written in Python for automatic C/S O&M. One of the two discovered vulnerabilities is authentication bypass vulnerabilities (CVE-2020-11651), and the other is directory traversal vulnerability (CVE-2020-11652). Attackers can exploit the vulnerabilities to remotely execute commands, read any files on the server, and obtain sensitive information.

If you are a SaltStack user, check your system and implement timely security hardening.

Vulnerability ID

- CVE-2020-11651
- CVE-2020-11652

Vulnerability Name

SaltStack remote command execution vulnerability

Scope of Impact

Affected versions:

- Versions earlier than SaltStack 2019.2.4
- Versions earlier than SaltStack 3000.2

Unaffected versions:

- SaltStack 2019.2.4
- SaltStack 3000.2

Official Solution

- These vulnerabilities have been fixed in the latest official version. If your service version falls into the affected range, upgrade it to the latest secure version.

 Download address: **https://repo.saltstack.com**

- The default listening ports of Salt Master are 4505 and 4506. You can configure security group rules that prohibit opening the two ports to public networks, or only allow trusted objects to connect to the ports.

Suggestion

Perform the following steps to scan and fix a vulnerability.

- Detect and view system details. For details, see **Viewing Vulnerability Details**.

  Fix vulnerabilities and verify the result. For details, see **Handling Vulnerabilities**..

Figure 2-2 Manually starting a vulnerability scan
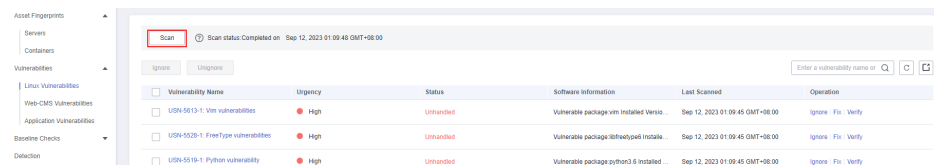
- Check whether ports 4505 and 4506 are enabled on the server.

  If ports 4505 and 4506 are enabled, you are advised to disable them or enable them only for trusted objects.

- Check for, isolate, and kill Trojans.

  Isolate and kill the mining Trojan. For details, see **Managing Isolated Files**.

Figure 2-3 Managing the isolated files
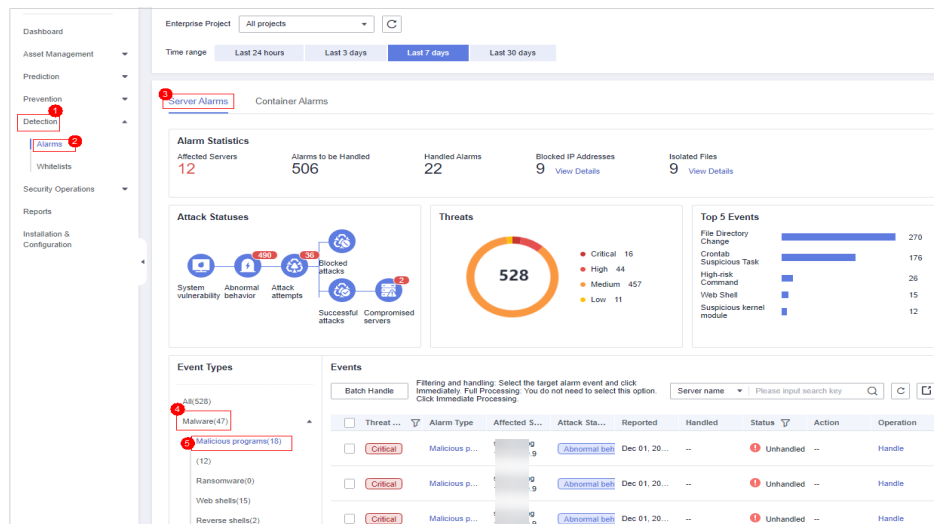
2.3 OpenSSL High-risk Vulnerability (CVE-2020-1967)

OpenSSL Project released update information regarding the OpenSSL vulnerability CVE-2020-1967 that affects OpenSSL 1.1.1d, OpenSSL 1.1.1e, and OpenSSL 1.1.1f. This vulnerability can be exploited to launch DDoS attacks.

Vulnerability ID

CVE-2020-1967

Vulnerability Name

OpenSSL high-risk vulnerability

Scope of Impact

- OpenSSL 1.1.1d
- OpenSSL 1.1.1e
- OpenSSL 1.1.1f

Official Solution

It is recommended that affected users install the latest vulnerability patch as soon as possible.

- **https://www.debian.org/security/2020/dsa-4661**
- **https://security.gentoo.org/glsa/202004-10**
- **https://lists.suse.com/pipermail/sle-security-updates/2020-April/006722.html**

Suggestion

Perform the following steps to scan and fix a vulnerability.

Step 1 Detect and view vulnerability details, as shown in **Manually starting a vulnerability scan**. For details, see **Viewing Vulnerability Details**.

Figure 2-4 Manually starting a vulnerability scan
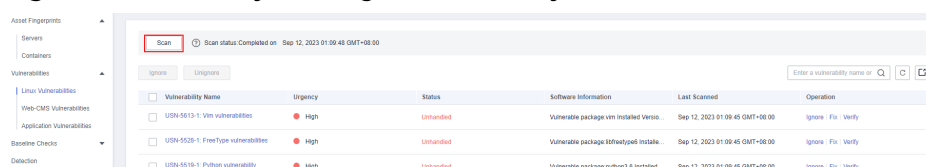
Step 2 Fix vulnerabilities and verify the result. For details, see **Handling Vulnerabilities**..

----End

2.4 Adobe Font Manager Library Remote Code Execution Vulnerability (CVE-2020-1020/CVE-2020-0938)

A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.

For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely. For systems running Windows 10, an

attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox context with limited privileges and capabilities. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

There are multiple ways an attacker could exploit the vulnerability, such as convincing a user to open a specially crafted document or viewing it in the Windows Preview pane.

Vulnerability ID

- CVE-2020-1020
- CVE-2020-0938

Vulnerability Name

Adobe Font Manager Library Remote Code Execution Vulnerability

Vulnerability Details

- For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely.
- For systems running Windows 10, an attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox context with limited privileges and capabilities. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Scope of Impact

All Windows OSs

Official Solution

It is recommended that affected users install the latest vulnerability patch as soon as possible.
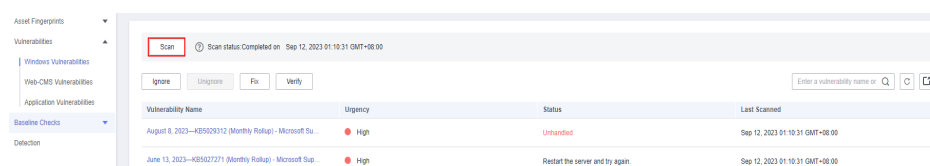
For details, see https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1020.

Suggestion

Perform the following steps to scan and fix a vulnerability.

Step 1 Detect and view vulnerability details. For details, see **Viewing Vulnerability Details**.

Figure 2-5 Manually starting a vulnerability scan

Step 2 Fix vulnerabilities and verify the result. For details, see **Handling Vulnerabilities**..

----End

2.5 Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027)

An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.

To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.

Vulnerability ID

CVE-2020-1027

Vulnerability Name

Windows Kernel Elevation of Privilege Vulnerability

Vulnerability Details

An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.

Affected Versions

All Windows OSs

Official Solution

It is recommended that affected users install the latest vulnerability patch as soon as possible.
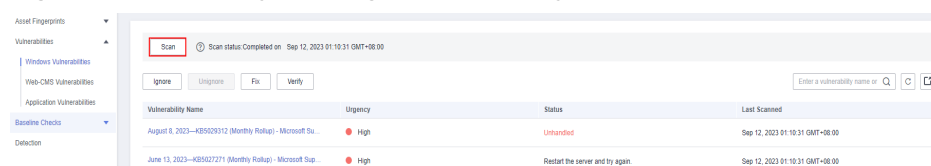
For details, see https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1027.

Suggestion

Perform the following steps to scan and fix a vulnerability.

Step 1 Detect and view vulnerability details. For details, see **Viewing Vulnerability Details**.

Figure 2-6 Manually starting a vulnerability scan

Step 2 Fix vulnerabilities and verify the result. For details, see **Handling Vulnerabilities**..

----End

2.6 Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)

On January 15, 2020, Microsoft released a patch update list, which contains the high-risk vulnerability CVE-2020-0601 that is discovered by National Security Agency (NSA) and affects Microsoft Windows encryption. This vulnerability affects the CryptoAPI Elliptic Curve Cryptography (ECC) certificate validation mechanism. As a result, attackers can interrupt the Windows authentication and encryption trust process and remotely execute code.

Vulnerability ID

CVE-2020-0601

Vulnerability Name

Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)

Vulnerability Details

A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates ECC certificates.

An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable file. The file appears to be from trusted and legitimate sources, and the user cannot know it is malicious. For example, an attacker could exploit this vulnerability to give seemingly trusted signature certificates to malware, such as ransomware, and bypass the Windows trust detection mechanism and mislead users to install the malware.

A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software. Instances that affect Windows trust relationships include common HTTPS connections, file signatures, and email signatures.

Affected Versions

- Windows 10
- Windows Server 2016 and Windows Server 2019
- Applications that depend on Windows CryptoAPI

Official Solution

It is recommended that affected users install the latest vulnerability patch as soon as possible.

For details, see https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-0601.

Suggestion

Perform the following steps to scan and fix a vulnerability.

Ensure you have installed the Host Security Service agent on the server to be fixed, and has enabled protection.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Servers & Quota**. In the server list, click the name of a Windows server to view its details.

Step 4 On the details page, choose **Vulnerabilities** > **Windows Vulnerabilities** and click **Scan**.

Figure 2-7 Manually starting a vulnerability scan
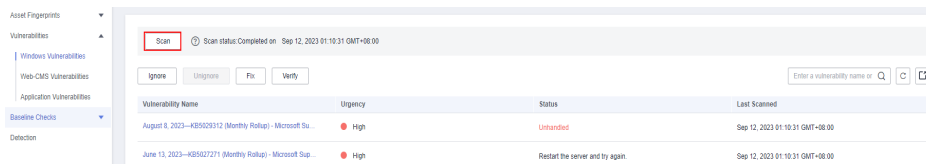
Step 5 Fix detected vulnerabilities according to the suggestion in the **Solution** column.

Step 6 Restart the fixed servers.

Step 7 Click **Manual Detection** again to check whether the vulnerabilities have been fixed.

> **◯ NOTE**
>
> You can also choose **Vulnerabilities** and click **Windows Vulnerabilities**, search for a vulnerability by its name, and then check and fix the vulnerability.
>
> - Windows Server 2019: KB4534273
> - Windows Server 2016: KB4534271

----End

3 HSS Multi-Cloud Management and Deployment

3.1 Application Scenario

With the development of hybrid clouds, there is also a growing need for companies to perform unified security management on hybrid clouds. HSS supports multiple cloud platforms and provides a complete set of security operation management solutions for hybrid clouds. It helps companies reduce service security risks in the hybrid cloud architecture through unified views, experience, and management, improving the overall security operation efficiency.

Scenario

To monitor workloads and centrally manage resources of the clouds, on-premises, and on hybrid clouds, HSS provides a security solution that helps you manage Huawei Cloud and hybrid clouds in a unified manner. HSS allows you to use the same security policies on different clouds, preventing the risks caused by inconsistent security policies.

Huawei Cloud solution

On the Huawei Cloud HSS console, you can centrally manage your Huawei Cloud servers, data centers, edge clouds, and other clouds.

Hybrid cloud solution

On the hybrid cloud HSS console, you can centrally manage your Huawei Cloud servers, data centers, edge clouds, and other clouds.
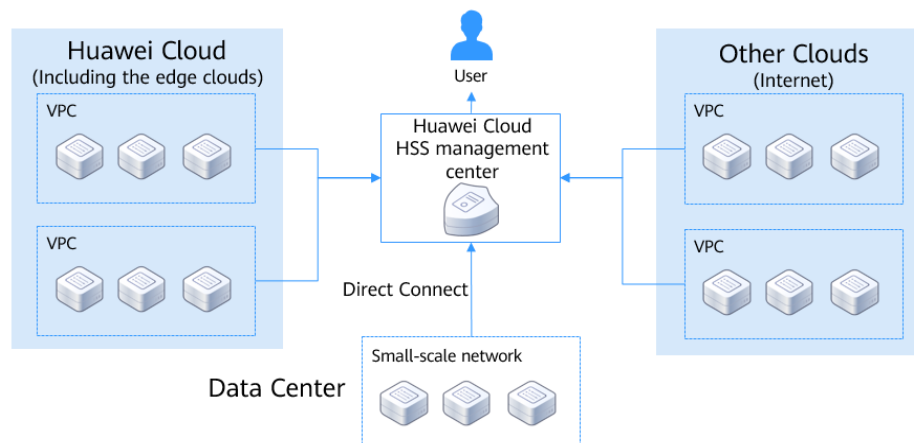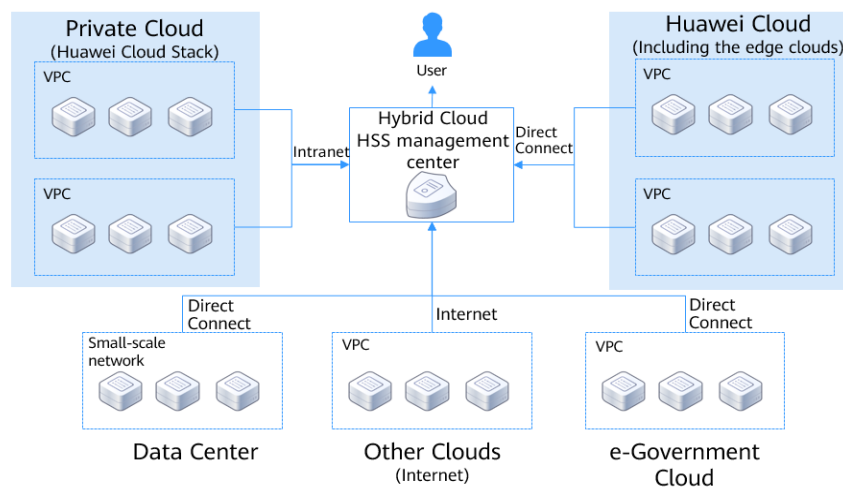
Figure 3-1 Huawei Cloud solution

Figure 3-2 Hybrid cloud solution

3.2 Installation and Deployment Process

If you want to centrally manage your servers on the Huawei Cloud or hybrid cloud HSS management console, and your servers include Huawei Cloud servers, non-Huawei Cloud servers (accessed over the Internet), and LAN servers (in data centers and on e-Government clouds), you need to install agents on your servers in sequence based on their application scenarios.

Huawei Cloud Solutions

The methods and commands used for installing agents vary according to the server types.

Table 3-1 Commands for installing the Huawei Cloud solution

Server Type	How to Obtain
Huawei Cloud server	Copy the Huawei Cloud installation commands on the Huawei Cloud console.
Non-Huawei Cloud server (Internet)	Copy the non-Huawei Cloud installation commands on the Huawei Cloud console.
LAN server (including data centers and e-Government clouds)	Set up a proxy and generate the installation command or package. Using a direct connect proxy server can avoid accessing public network.

For details about how to install Huawei Cloud and non-Huawei Cloud servers (Internet), see **Installing an Agent**. For details about how to install LAN servers (including data centers and e-Government clouds), see **Figure 3-3**.

Figure 3-3 Deployment on a LAN server
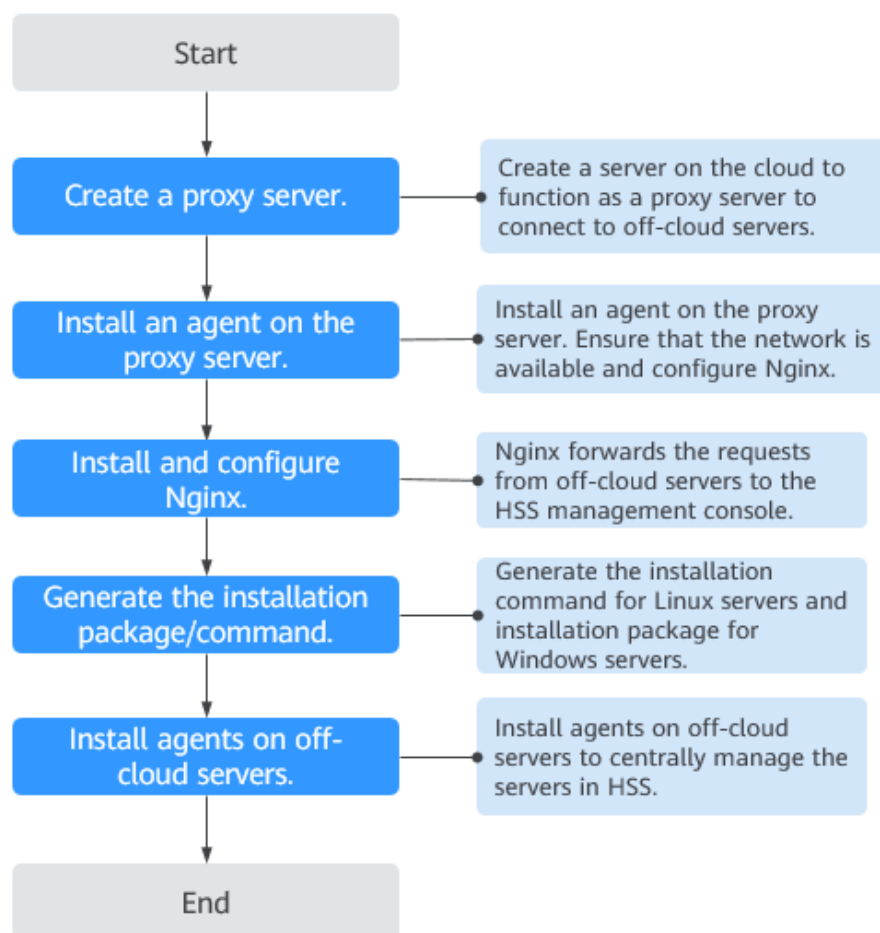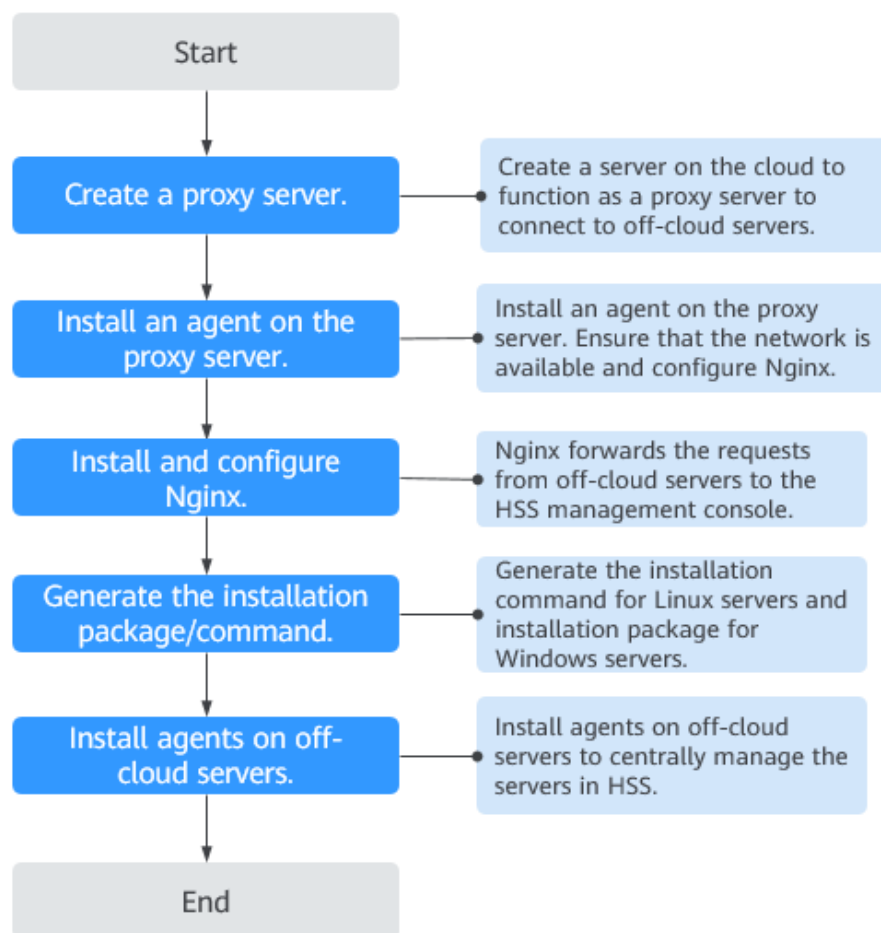
Hybrid Cloud Solution

The methods and commands used for installing agents vary according to the server types.

Table 3-2 Installation commands for the hybrid cloud solution

Server Type	How to Obtain
Huawei Cloud server	Copy the Huawei Cloud installation commands on the Huawei Cloud console.
Non-Huawei Cloud server (Internet)	Set up a proxy and generate the installation commands or packages. Using a direct connect proxy server can avoid accessing public network.
LAN server (including data centers and e-Government clouds)	

For details about how to install Huawei Cloud servers, see **Installing the Agent**. For details about how to install non-Huawei Cloud servers (Internet) and LAN servers (including data centers and e-Government clouds), see **Figure 3-4**.

Figure 3-4 Deployment on a LAN server

3.3 Installation and Deployment

3.3.1 Huawei Cloud Solutions

You can use HSS to centrally manage your servers. If your server types include Huawei Cloud servers, non-Huawei Cloud servers (Internet), and LAN servers (including data center and e-Government cloud servers), install agents on the servers based on the server type.

Huawei Cloud Server/Non-Huawei Server (Internet)

- To manage Huawei Cloud and non-Huawei Cloud servers (Internet) on the HSS console, you can directly install agents on the servers in the target region.
  - For details about how to install an agent on a Linux Huawei Cloud or non-Huawei Cloud server (Internet), see **Installing an Agent on Linux**.
  - For details about how to install an agent on a Windows Huawei Cloud or non-Huawei Cloud server (Internet), see **Installing an Agent on Windows**.

LAN Server (Data Center, e-Government Cloud, Private Cloud)

To centrally manage LAN servers in the Huawei Cloud HSS console, create a proxy server that uses Direct Connect, manually create the agent installation command (or package), and install agents on your servers.

For details, see **Connecting Off-cloud Servers to the Public Cloud Through Direct Connect**.

3.3.2 Hybrid Cloud Solution

You can use hybrid HSS to centrally manage your servers. If your server types include Huawei Cloud servers, non-Huawei Cloud servers (Internet), and LAN servers (including data center and e-Government cloud servers), install agents on the servers based on the server type.

Huawei Cloud Server

To manage Huawei Cloud servers on the hybrid cloud HSS console, you can directly install agents on the servers in the target region.

- For details about how to install the agent on a Linux Huawei Cloud server, see **Installing an Agent on Linux**.
- For details about how to install the agent on a Windows Huawei Cloud server, see **Installing an Agent on Windows**.

Non-Huawei Server (Internet)/LAN Server (Data Center, e-Government Cloud, Private Cloud)

To centrally manage non-Huawei Cloud servers (Internet) and LAN servers in the hybrid cloud HSS console, create a proxy server that uses Direct Connect, manually

create the agent installation commands (or packages), and install the agents on the servers.

For details, see **Connecting Off-cloud Servers to the Public Cloud Through Direct Connect**.

3.4 Verification and Usage

After the installation is complete, log in to Huawei Cloud or hybrid cloud HSS console and go to the ECS list page. If the target ECS is displayed in the list, the offline ECSs have been connected to the HSS console and managed in a unified manner.

◫ NOTE

- After the installation is complete, ensure that port 10180 of the target server can be properly connected and the server is online.
- The server status is not displayed after non-Huawei servers (Internet) and LAN servers (such as data centers, e-Government clouds, and private clouds) are connected to the HSS console.

3.5 Connecting Off-cloud Servers to the Public Cloud Through Direct Connect

3.5.1 Step 1: Creating a Proxy Server

Create a server on the cloud to function as a proxy server to connect to off-cloud servers.

Procedure

Log in to the Huawei Cloud management console and purchase an ECS. For details, see **Purchasing an ECS**.

NOTICE

- The CPU architecture of the proxy server must be x86.
- The number of vCPUs of the proxy server must be 4 or greater, and the memory must be 8 GiB or greater.
- Set the proxy server image to **Public Image** and **openEuler 20.03 64bit**.

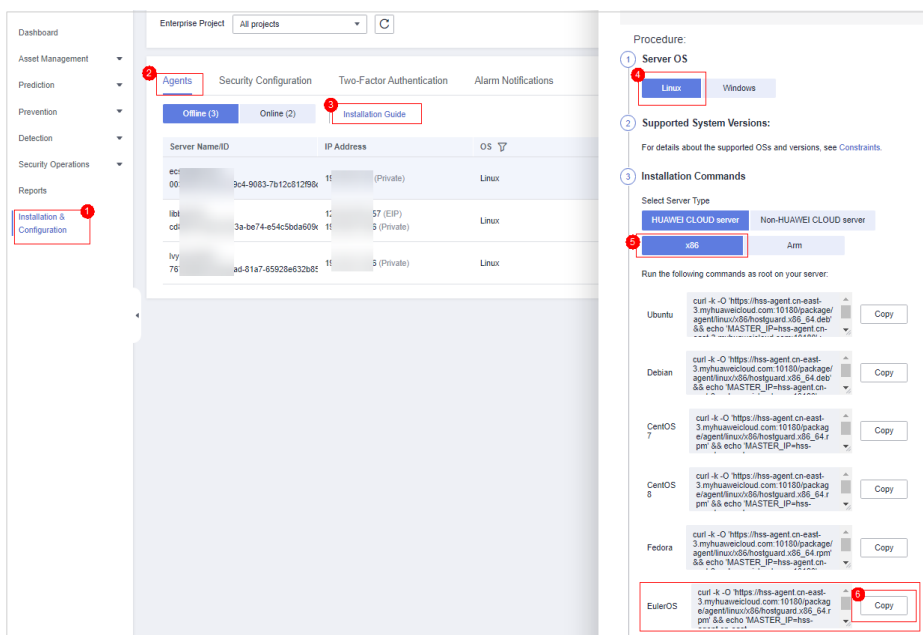
Figure 3-5 Creating a proxy server
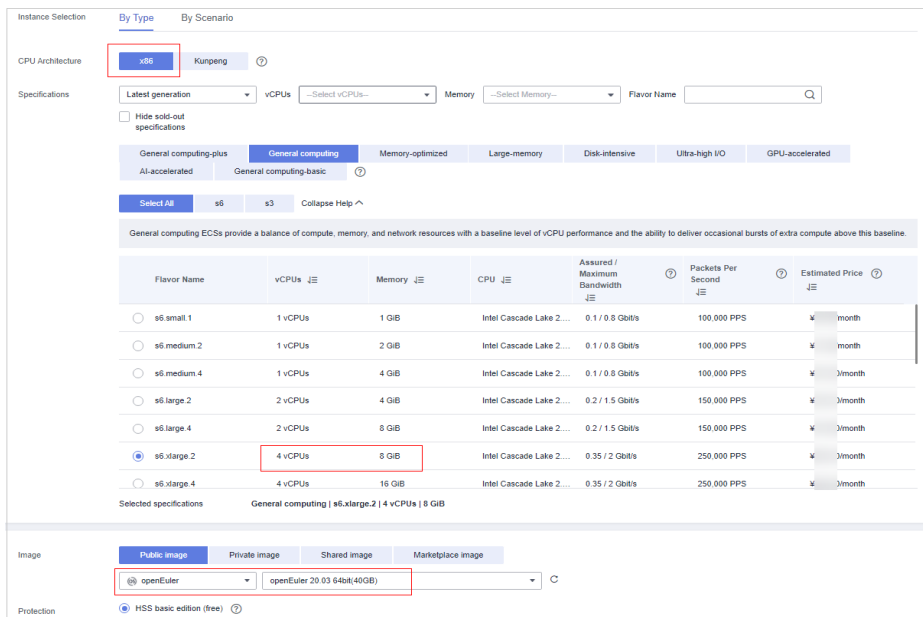
3.5.2 Step 2: Installing an Agent for the Proxy Server

Install an agent on the proxy server. Ensure the network is available and configure Nginx.

Procedure

Step 1 Log in to the HSS console (new), choose **Installation & Configuration**, and click **Agents** > **Add Asset from Other Cloud**. Select **Linux** and **x86**, and copy the installation commands of EulerOS.

Figure 3-6 Copying the installation command

Step 2 Log in to the proxy server and paste and run the copied commands to install the agent. For details, see **Installing an Agent on Linux**.

Figure 3-7 Installing an agent

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

Step 3 About 10 minutes later, go to the ECS list page and check whether **Agent Status** of the proxy server is **Online**.

> **NOTICE**
>
> Ensure that the agent server is online before performing subsequent steps. Otherwise, subsequent steps may fail.

----End

3.5.3 Step 3: Installing and Configuring Nginx

Nginx forwards requests from off-cloud servers to the HSS management console.

Preparation: Checking the Yum Repository

Check whether the Nginx software package exists in the Yum repository. If the Nginx software package does not exist, configure the Yum repository and bind the public IP address temporarily. After the installation is complete, unbind the public IP address.

Step 1 Remotely log in to the proxy server and run the following command to check whether the Nginx package exists in the Yum repository:

yum list nginx

Step 2 If the information shown in **Figure 3-8** is displayed, the Nginx package exists.

Figure 3-8 The Nginx package exists

```
[root@hssnginx ~]# yum list nginx
OS                                                          1.2 MB/s | 2.7 MB     00:02
everything                                                  4.2 MB/s | 9.1 MB     00:02
EPOL                                                        723 kB/s | 911 kB     00:01
debuginfo                                                   1.7 MB/s | 2.8 MB     00:01
source                                                      1.5 MB/s | 816 kB     00:00
Available Packages
nginx.src                                    1:1.16.1-2.oe1                           source
nginx.x86_64                                 1:1.16.1-2.oe1                           everything
[root@hssnginx ~]#
```

----End

Installing Nginx

Step 1 Run the following command to install Nginx using Yum:

yum install -y nginx

Figure 3-9 Installing Nginx

Step 2 Nginx is automatically installed. If **Complete!** shown in **Figure 3-10** is displayed, the installation is successful.

Figure 3-10 Nginx installed successfully

----End

Configuring Nginx

Step 1 Run the following command to go to the Nginx directory:

cd /etc/nginx/

Step 2 Run the following command to sign the certificate:

openssl req –new –x509 –nodes –out server.pem –keyout server.key –days 36500

After the command is executed, enter the certificate information.

Figure 3-11 Self-signed certificate

📖 NOTE

The value of **Country Name** can contain only two characters.
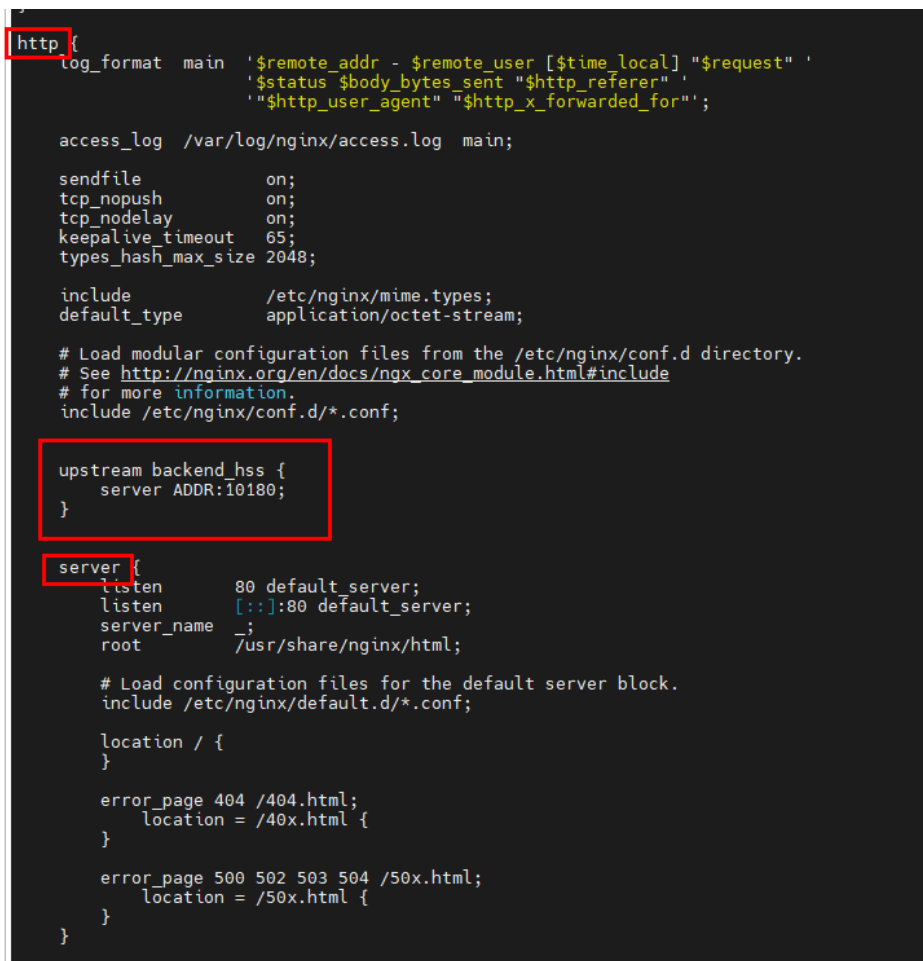
Step 3 Run the following command to modify **nginx.conf**:

vi nginx.conf

Step 4 Configure **upstream**. Find **server** under **http** and add the following information above **server**:

upstream backend_hss {

server ADDR:10180;

}

Figure 3-12 Configuring upstream

Step 5 Configure **server**. Retain one **listen** record under the listening port and change the value to **10180**. Change the value of **server_name** to **ADDR**.

Figure 3-13 Configuring server


```
upstream backend_hss {
    server ADDR:10180;
}


server {
    listen        10180;

    server_name  ADDR;
    root         /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    location / {
    }

    error_page 404 /404.html;
        location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
        location = /50x.html {
    }
}
```

Step 6 Add the following information under **server** to enable SSL authentication:

ssl on;

ssl_protocols TLSv1.2;

ssl_certificate "server.pem";

ssl_certificate_key "server.key";

ssl_session_cache shared:ssl:10m;

ssl_session_timeout 10m;

ssl_prefer_server_ciphers on;

Figure 3-14 Enabling SSL authentication


```
server {
    listen        10180;

    server_name  ADDR;
    root          /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    ssl     on;
    ssl_protocols   TLSv1.2;
    ssl_certificate "server.pem";
    ssl_certificate_key "server.key";
    ssl_session_cache shared:SSL:10m;
    ssl_session_timeout  10m;
    ssl_prefer_server_ciphers on;

    location / {
    }

    error_page 404 /404.html;
        location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
        location = /50x.html {
    }
}
```

Step 7 Configure **location**. Find **location** under **server** and add the following information to **{}** under **location**:

limit_except GET POST PUT

{

deny all;

}

proxy_set_header Host ADDR;

proxy_pass https://backend_hss;

proxy_set_header Upgrade $http_upgrade;

proxy_set_header Connection "upgrade";

Figure 3-15 Configuring location


```
server {
    listen        10180;

    server_name  ADDR;
    root         /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    ssl    on;
    ssl_protocols   TLSv1.2;
    ssl_certificate "server.pem";
    ssl_certificate_key "server.key";
    ssl_session_cache shared:SSL:10m;
    ssl_session_timeout  10m;
    ssl_prefer_server_ciphers on;

    location / {
        limit_except GET POST PUT
        {
            deny all;
        }
        proxy_set_header Host ADDR;
        proxy_pass https://backend_hss;

        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";

    }

    error_page 404 /404.html;
        location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
        location = /50x.html {
    }
}
```

Step 8 **Optional:** Enter **ECS**, run the following command, and press **Enter** to exit.

:wq!

Figure 3-16 Saving the settings and exiting

Step 9 Run the following commands in sequence to start Nginx:

sed -i "s#ADDR#`cat /usr/local/hostguard/conf/connect.conf | grep master_address | cut -d '=' -f 2 | cut -d ':' -f 1`#g" nginx.conf

echo '*/10 * * * * root systemctl start nginx' >> /etc/crontab

systemctl start nginx

----End

3.5.4 Step 4: Generating an Installation Package/Command

Generate the installation command for Linux servers and the package for Windows servers.

Generating the Installation Command for Linux Servers

Step 1 Run the following command to access the **/tmp** directory:

cd /tmp

Step 2 Run the following commands in sequence to check whether the IP address in **private_ip.conf** is available:

echo `hostname -I` > private_ip.conf

cat private_ip.conf

Figure 3-17 Checking the IP address

NOTICE

- Check whether the IP address in **private_ip.conf** is available for the proxy server. Ensure that the IP address can be connected by off-cloud servers.

- If the IP address is not available, manually change it.

Step 3 After confirming that the IP address is available, run the following commands in sequence to generate the installation command:

- x86 RPM software package image:

  echo -e "# for Liunx x86 CentOS EulerOS OpenSUSE Fedora\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.rpm' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && rpm -ivh hostguard.x86_64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm" > x86_rpm_install.sh

- x86 deb software package image:

  echo -e "# for Liunx x86 Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.x86_64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > x86_deb_install.sh

- ARM RPM software package image:

  echo -e "# for Liunx ARM CentOS EulerOS OpenSUSE Fedora UOS Kylin\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.rpm' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && rpm -ivh hostguard.aarch64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm" > arm_rpm_install.sh

- ARM deb software package image:

  echo -e "# for Liunx ARM Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.aarch64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > arm_deb_install.sh

- Change to an available IP address:

sed -i "s#private_ip#`cat private_ip.conf`#g" *install.sh && sed -i "s#project_id#`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2`#g" *install.sh

📖 **NOTE**

- All the five commands must be executed. The last command that is used to change to an available IP address must be executed at last.

- The installation commands in **x86_rpm_install.sh** are suitable for images managed by the RPM software package in the x86 architecture, such as CentOS, EulerOS, OpenSUSE, and Fedora.

- The installation commands in **x86_deb_install.sh** are suitable for images managed by the .deb software package in the x86 architecture, such as Ubuntu and Debian.

- The installation commands in **arm_rpm_install.sh** are suitable for images managed by the RPM software package in the ARM architecture, such as CentOS, EulerOS, OpenSUSE, Fedora, UOS, and Kylin.

- The installation commands in **arm_deb_install.sh** are suitable for images managed by the .deb software package in the ARM architecture, such as Ubuntu and Debian.

Step 4 View the generated installation command, which will be used to install agents on the off-cloud Linux servers.

Figure 3-18 Linux installation commands

----End

Generating the Installation Package for Windows Servers

Step 1 Run the following command to access the **/tmp** directory:

cd /tmp

Step 2 Run the following commands in sequence to generate the agent installation package for Windows servers:

curl -k -O https://`cat private_ip.conf`:10180/package/agent/windows/hostguard_setup.exe && echo '[system]' > hostguard_setup_config.ini && echo 'master=`cat private_ip.conf`:10180' >> hostguard_setup_config.ini && echo 'slave=`cat private_ip.conf`:10180' >> hostguard_setup_config.ini && echo 'orgid=`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2`' >> hostguard_setup_config.ini

zip hostguard_setup.zip hostguard_setup.exe hostguard_setup_config.ini

📖 **NOTE**

> If the proxy server does not have zip commands, run the following command to install the zip plugin:
>
> yum install -y zip

Step 3 View the generated installation package, which will be used to install agents on the off-cloud Windows servers.

Figure 3-19 Windows installation package

----End

3.5.5 Step 5: Installing Agents on Off-cloud Servers

Install agents on off-cloud servers and manage the servers in HSS in a unified manner.

Installing Agents on Off-cloud Linux Servers

Log in to an off-cloud server and copy the command generated in **Generating Installation Commands for Linux Servers** to the server to install an agent.

For details, see step 8 in **Installing an Agent on Linux**.

Installing Agents on Off-cloud Windows Servers

Copy the **hostguard_setup.zip** package generated in **Generating Installation Packages for Linux Servers** to the local PC and upload it to an off-cloud Windows server to install the agent. Decompress the installation package and double-click **hostguard_setup.exe** to install the agent.

NOTICE

After the generated .zip installation package is copied to the local PC, you must decompress the package before installing the software. Otherwise, the installation will fail.

4 Best Practices for Defense Against Ransomware

4.1 What Is a Ransomware Attack?

Ransomware attacks have become one of the biggest security challenges facing companies today. Ransomware is a type of malware attack in which the attacker locks the victim's data or asset devices and then demands a payment to unlock the data. Sometimes, attackers may not unlock the data even after receiving the ransom.

Ransomware attacks can cause interruption to your services and the leakage or loss of critical information and data. As a result, the operation, economy, and reputation of your company may be greatly affected and security problems may hinder your company development.

With ransomware attacks spiking in recent years, this malware is evolving to become stealthier, faster, and more impactful. Defending against ransomware attacks is now a major and urgent task for companies.

Figure 4-1 Ransomware overview

4.2 Process of Ransomware Attacks

When attacking cloud infrastructure, attackers usually attack multiple resources in an attempt to obtain access to customer data or company secrets. The process of

a ransomware attack can be divided into three stages: investigation and detection, intrusion and lateral movement, and extortion.

- **Intrusion**: Attackers collect basic information, look for attack vectors, enter the environment, and establish an internal foothold.

- **Lateral movement**: Attackers deploy attack resources, detect network assets, elevate access permissions, steal credentials, implant ransomware, damage the detection and defense mechanism, and expand the attack scope.

- **Encryption extortion**: Attackers steal confidential data, encrypt key data, load ransomware information, and ask for ransom.

Figure 4-2 Extortion process
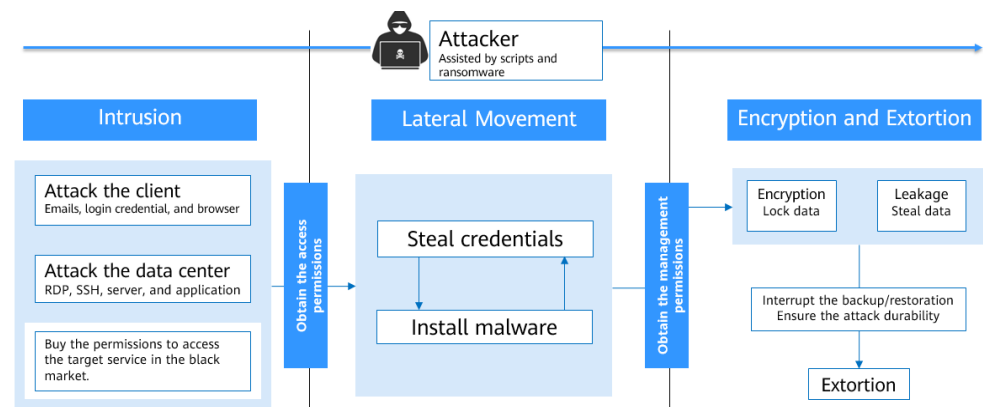
4.3 Protecting Against Ransomware (General Actions)

Pre-event Measures

It is difficult to decrypt the data that has been encrypted by ransomware, or to track attackers based on their digital currency transactions. The most effective way to fight ransomware attacks is to improve anti-attack capabilities.

You are advised to perform the following operations to protect your servers against ransomware:

- **Minimize the scope exposed to the Internet**: Periodically scan external ports and ensure only necessary ports are enabled.

- **Reduce system risks**: Periodically scan vulnerabilities and system risk configuration parameters to fix vulnerabilities and risks in a timely manner. In addition, pay attention to the security vulnerability information and patch information released by software vendors, and manage and fix vulnerabilities in a timely manner.

- **Enhance network access control**: Clearly define network security zones and access control rules, minimize access rights, and update access control rules in a timely manner.

- **Back up important data**: Reliable data backup can minimize the loss caused by ransomware. Encrypt the storage and periodically back up critical service data, and set proper backup retention rules to ensure that valid copies can be used to restore data once being attacked.

- **Enhance account permission control**: Assign accounts and permissions to different roles based on access control rules such as identity management and fine-grained permission control. Improve the security of privileged accounts. Properly set and save accounts and passwords for key service assets of your company. Configure two-factor authentication to identify the personnel that access key assets and reduce brute-force cracking risks.

- **Establish high-reliability service architecture**: Deploy cloud services in cluster mode. If an emergency occurs on a node, services will be switched to the standby node, improving reliability and preventing data loss. If you have sufficient resources, you can build intra-city or remote DR and backup systems. If the primary system is attacked by ransomware, your services can be quickly switched to the backup system and will not be interrupted.

- **Develop emergency plans for security incidents**: Establish an emergency organization and management mechanism to deal with cybersecurity incidents such as ransomware attacks, and specify work principles, division of responsibilities, emergency handling processes, and key measures. Once your service is attacked by ransomware, immediately start the internal cyber security emergency plan and carry out standardized emergency handling to mitigate and eliminate the impact of the ransomware attack.

- **Enhance employees' security awareness**: Improve employees' cyber security awareness through training and drills. Ensure that employees understand national cyber security laws and regulations and Huawei cyber security regulations, can identify common cyber security attacks such as phishing, have certain incident handling capabilities, and know the consequences and impacts of security incidents.

In-event Measures

When an intruder bypasses the defense mechanism, if you can detect and block the intruder in a timely manner, a disaster can be avoided.

You are advised to perform the following operations once being attacked by ransomware:

- **Rapidly isolate the infected devices**: Once being attacked, immediately disconnect the network or power off the system to prevent the spread of the ransomware attack. Change the passwords of infected devices and other devices on the same LAN in a timely manner.

- **Quickly handle the intrusion events**: Perform real-time security scan on service resources, isolate and block the ransomware, block the source IP addresses of the ransomware and the IP addresses suspected of brute-force attacks, and block the running, communication, and connection of the ransomware.

Post-event Measures

Currently, ransomware attacks develop rapidly and no tools can provide 100% protection. Once being attacked, restore your services in a timely manner and harden network security to reduce the impact of the ransomware attacks.

You are advised to perform the following restoration operations:

- **Use backup data to restore services**: Determine the data restoration scope, sequence, and backup version based on the backup status of the attacked device, and use the backup data to restore services.
- **Check and fix network risks**: Identify system vulnerabilities based on ransomware attack paths. Check and fix the system vulnerabilities.

4.4 Huawei Cloud Ransomware Prevention Solution (HSS+CBR)

4.4.1 Overview

In addition to the general actions for protecting against ransomware (**Protecting Against Ransomware (General Actions)**), both HSS and CBR can improve your comprehensive ransomware defense capability.

Currently, ransomware is frequently upgraded and evolved. HSS can detect ransomware and identify system risks, but it cannot provide protection against 100% of the viruses out there. You can use CBR to improve ransomware prevention capabilities and reduce the impact of ransomware attacks. If only CBR is configured, the system may fail to restore the data generated between the last backup and the ransomware attack. You can use HSS to detect ransomware in real time and minimize data loss. Therefore, you are advised to use both HSS and CBR to protect companies before, during, and after ransomware attacks.

- **Pre-event: Quickly Detect and Resolve Ransomware Attacks**

  For details, see **Identifying and Fixing Ransomware**.

- **In-event: Detect, Isolate, and Block Ransomware Attacks in Real Time**

  For details, see **Enabling Ransomware Prevention and Backup**.

- **Post-event: Minimize Losses and Quickly Recover Services**

  For details, see **Restoring Server Data**.

Ransomware Protection Configuration

According to Huawei Cloud security event statistics, using HSS and CBR together can greatly improve your comprehensive ransomware defense capabilities. To provide strongest ransomware protection with these services, you are advised to enable the ransomware protection policy of the HSS premium edition and enable and configure hour-level permanent CBR backup.

Host Security Service (HSS)	Cloud Backup and Recovery (CBR)	Encryption Probability	Recovery Probability	Ransomware Protection Rating (0-100)

Edition	Ransomware Protection Policy	Configuration Status	Shortest Backup Period (Recommended)			
-	-	-	-	High (90%)	0%	0
Basic edition	Not supported	-	-	High (90%)	0%	0
Enterprise edition	Not supported	-	-	High (85%)	0%	10
Premium edition	Unconfigured	-	-	Medium (50%)	0%	15
Basic edition /Not enabled	Not supported	Configured	Day	High (90%)	50%	20
Enterprise edition	Not supported	Configured	Day	High (85%)	50%	30
Basic edition /Not enabled	Not supported	Configured	Hour	High (90%)	90%	30
Premium edition	Unconfigured	Configured	Day	Medium (50%)	50%	35
Enterprise edition	Not supported	Configured	Hour	High (85%)	90%	40
Premium edition	Unconfigured	Configured	Hour	Medium (50%)	90%	45
Premium edition	Configured	-	-	Low (< 10%)	0%	60

Premium edition	Configured	Configured	Day	Low (< 10%)	50%	80
Premium edition	Configured	Configured	Hour	Low (< 10%)	90%	90
Premium edition	**Configured**	**Configured**	**Hour (Permanent backup)**	**Low (< 10%)**	**90%**	**99 (Recommended)**

4.4.2 Identifying and Fixing Ransomware

Once being attacked by ransomware, we need to identify and isolate ransomware and back up and restore service data in a timely manner. Huawei Cloud Host Security Service uses ransomware detection engines and dynamic honeypots to prevent ransomware from intruding your system, encrypting data, or spreading to other devices. HSS can detect and remove ransomware in seconds, back up and recover service data in minutes, and provide industry-leading ransomware prevention and control capabilities.

According to the statistics of Huawei Cloud on security intrusion events, 90% of ransomware attacks are results of weak passwords, vulnerability exploits, and unsafe baseline settings. Identifying and fixing risks before real intrusions can significantly improve the system security. Huawei Cloud Host Security Service helps you quickly identify risks and provides one-click repair to reduce enterprise O&M costs.

Increasing Password Strength

HSS automatically scans servers every early morning for common weak passwords and **the passwords you banned**. You can then ask the weak password users to set stronger passwords. HSS can detect weak passwords in SSH, FTP, and MySQL.

Step 1 Log in to the management console.

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

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

Step 4 Click the **Common Weak Password Detection** tab to view the weak passwords of the server.

Step 5 Log in to servers to harden weak passwords based on the server names, account names, and account types corresponding to the detected weak passwords.

After hardening weak passwords, you are advised to perform **manual scan** immediately.

----End

Hardening Baseline Configurations

HSS scans your software for unsafe settings every early morning and provides suggestions. You can modify your settings accordingly to enhance server security.

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, choose **Prediction** > **Baseline Checks**.

Step 3 Click the **Unsafe Configurations** tab to view the unsafe configurations of the server.

Step 4 Click the target baseline name. The baseline details page is displayed.

Step 5 Click the **Check Items** tab and click **Failed** to view baseline risk items.

Step 6 Click **View Details** in the **Operation** column of a check item to view the modification suggestions and affected servers.

Step 7 Log in to the affected server and harden the configuration based on the modification suggestions.

Step 8 After hardening a configuration, click **Verify** in the **Operation** column to verify the hardening result.

> ☐ **NOTE**
>
> You are advised to repeat the preceding steps to fix all high-risk configurations.

----End

Fixing Vulnerabilities

By default, HSS automatically performs a comprehensive vulnerability detection every week and provides fixing suggestions. You can fix the vulnerabilities based on the suggestions. You can also configure the automatic vulnerability detection period. For details, see .

> ☐ **NOTE**
>
> There are four levels of vulnerability fix priorities: critical, high, medium, and low. You are advised to fix vulnerabilities of the critical and high levels promptly and fix vulnerabilities of the medium and low levels based on service requirements.

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, choose **Prediction** > **Vulnerabilities**. The vulnerability management page is displayed.

Step 3 Click the **Linux Vulnerabilities**, **Windows Vulnerabilities**, **Web-CMS Vulnerabilities**, and **Application Vulnerabilities** tabs to view the vulnerabilities of the server.

Step 4 Fix vulnerabilities based on vulnerability types.

- Linux and Windows vulnerabilities

  In the row of the vulnerability you want to fix, click **Fix** in the **Operation** column.

  You can also select multiple vulnerabilities and click **Fix** in the upper left corner of the vulnerability list to fix them in batches.

- Web-CMS vulnerabilities and application vulnerabilities

  a. Click a vulnerability name to view vulnerability fixing suggestions.

  b. Log in to the server affected by the vulnerability and manually fix the vulnerability.

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

     - Method 1: Create a new VM to fix the vulnerability.

       1) Create an image for the ECS to be fixed.

          For details, see **Creating a Full-ECS Image from an ECS**.

       2) Use the image to create an ECS.

          For details, see **Creating an ECS from an Image**.

       3) Fix the vulnerability on the new ECS and verify the result.

       4) Switch services over to the new ECS and verify they are stably running.

       5) Release the original ECS.

          If a fault occurs after the service switchover and cannot be rectified, you can switch services back to the original ECS.

     - Method 2: Fix the vulnerability on the target server.

       1) Create a backup for the ECS to be fixed.

       2) Fix vulnerabilities on the current server.

       3) If services become unavailable after the vulnerability is fixed and cannot be recovered in a timely manner, use the backup to restore the server.

       📖 NOTE

       - Use method 1 if you are fixing a vulnerability for the first time and cannot estimate impact on services. In this way, you can release the ECS at any time to save costs if the vulnerability fails to be fixed.

       - Use method 2 if you have fixed the vulnerability on similar servers before.

  c. After a vulnerability is fixed, click the vulnerability name to go to the vulnerability details page.

  d. Click the **Affected** tab and choose **More** > **Verify** in the **Operation** column of an affected asset or IP address to verify the vulnerability fixing result.

  ----End

4.4.3 Enabling Ransomware Prevention and Backup

Once being attacked by ransomware, we need to identify and isolate ransomware and back up and restore service data in a timely manner. HSS uses ransomware detection engines and dynamic honeypots to prevent ransomware from intruding your system, encrypting data, or spreading to other devices. HSS can detect and remove ransomware in seconds, back up and recover service data in minutes, and provide industry-leading ransomware prevention and control capabilities.

You can enable ransomware prevention and backup to defend against ransomware attacks and reduce service loss risks, enhancing the ransomware prevention capabilities.

Step 1: Enabling Ransomware Prevention

If the version of the agent installed on the Linux server is 3.2.8 or later or the version of the agent installed on the Windows server is 4.0.16 or later, ransomware prevention is automatically enabled with the HSS premium, WTP, or container edition. If the agent version does not support the automatic enabling of ransomware prevention, you can manually enable it.

Step 1 Log in to the management console.

Step 2 Choose **Prevention** > **Ransomware Prevention**.

Step 3 Click the **Protected Servers** tab.

Step 4 In the **Ransomware Prevention Status** column of a server, click **Enable**.

You can also select multiple servers and click **Enable Ransomware Prevention** above the server list.

Step 5 In the **Enable Ransomware Prevention** dialog box, confirm the server information and select a protection policy.

Step 6 Click **OK**.

If the **Ransomware Prevention Status** of the server changes to **Enabled**, ransomware protection is enabled successfully.

----End

Step 2: Configuring a Ransomware Prevention Policy

Configure honeypot file directories, excluded directories, and protected file types based on service requirements.

Step 1 Log in to the management console.

Step 2 Choose **Prevention** > **Ransomware Prevention**.

Step 3 Click the **Protected Servers** tab.

Step 4 In the row of the target server, click the policy name in the **Policy** column. The **Edit Policy** page is displayed.

Step 5 Configure the policy information by referring to **Table 4-1**.

Table 4-1 Protection policy parameters

Parameter	Description	Example Value
OS	Server OS.	Linux
Policy	Policy name.	test

Parameter	Description	Example Value
Action	How an event is handled. ● **Report alarm and isolate** ● **Report alarm**	Report alarm and isolate
Honeypot File Directories	Directory that need to be protected by static bait (excluding subdirectories). You are advised to configure important service directories or data directories. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	Linux: **/etc** Windows: **C:\Test**
Excluded Directory (Optional)	Directory that does not need to be protected by bait files. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	Linux: **/etc/lesuo** Windows: C:\Test\ProData
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. This parameter is mandatory for Linux servers only.	Select all
(Optional) Process Whitelist	Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms. This parameter is mandatory only for Windows servers.	-

Step 6 Confirm the policy information and click **OK**.

----End

Step 3: Enabling Backup

To prevent service loss caused by ransomware attacks, enable the backup function for your servers to periodically back up service data.

☐ **NOTE**

If you do not have available vaults, purchase one by referring to and then enable the backup function.

Step 1 Log in to the management console.

Step 2 Choose **Prevention** > **Ransomware Prevention**.

Step 3 Click the **Protected Servers** tab.

Step 4 Select a server and click **Enable Backup** in the upper part of the server list.

Figure 4-3 Enabling backup
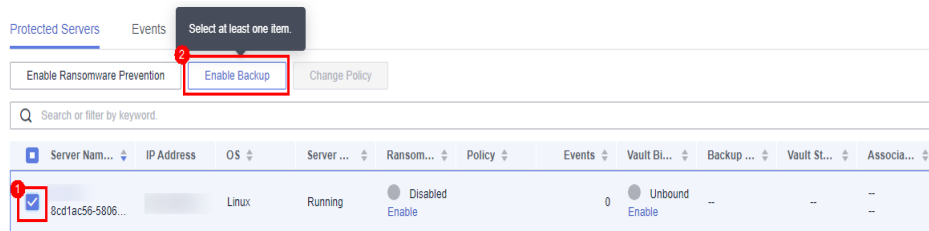
Step 5 In the **Enable Backup** dialog box, select a vault.

📖 NOTE

A vault that meets the following conditions can be bound:
● The vault is in **Available** or **Locked** state.
● The backup policy is in **Enabled** state.
● The vault has backup capacity available.
● The vault is bound to fewer than 256 servers.

Step 6 Click **OK**.

----**End**

4.4.4 Restoring Server Data

Currently, ransomware attacks develop rapidly and no tools can provide 100% protection. Backup and recovery can help you minimize the loss after ransomware attacks. Huawei Cloud CBR can quickly restore your services and ensure secure service running.

Before using the backup data to restore the service data of a server, check whether the backup is available. If the backup is available, restore the key service system first.

Procedure

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, choose **Prevention** > **Ransomware Prevention**. The ransomware prevention page is displayed.

Step 3 Click the **Protected Servers** tab.

Step 4 In the **Operation** column of the target server, click **More** > **Restore Data**.

Step 5 In the displayed **Backups** page, select the backup data you want to restore.

Step 6 In the **Operation** column of the target backup data, click **Restore Data**.

Step 7 In the displayed dialog page, confirm the server information and configure parameters such as the disk for storing data.

- **Restart the server immediately after restoration**: If you select this option, the server will be automatically restarted during data restoration.

- **Disk Backup**: Specify a storage disk for the data source you want to back up.

Step 8 Click **OK**.

----End

5 Installing the Host Security Service Agent Using CBH

Scenario

If you have purchased the Huawei Cloud Cloud Bastion Host (CBH) professional edition, you can use CBH to install the Host Security Service agent on your server. You do not need to obtain the server account and password or run complex installation commands. You can easily install the agent on one or more servers.

Prerequisites

- You have purchased the CBH professional edition and managed server resources through the CBH.

  For details, see **Purchasing a CBH Instance** and **Managing Host Resources Using CBH**.

- The server where the agent is to be installed is a Linux server of the SSH protocol type, and the network connection of the server is normal.

- You have obtained the system administrator account of the CBH.

Procedure

Step 1 Use the system administrator account to **Log In to the CBH System**.

Step 2 In the navigation tree on the left, choose **Operation** > **Fast Operation**. The **Fast Operation** page is displayed.

Step 3 Click the **Script Console** tab.

Figure 5-1 Accessing the Script Console
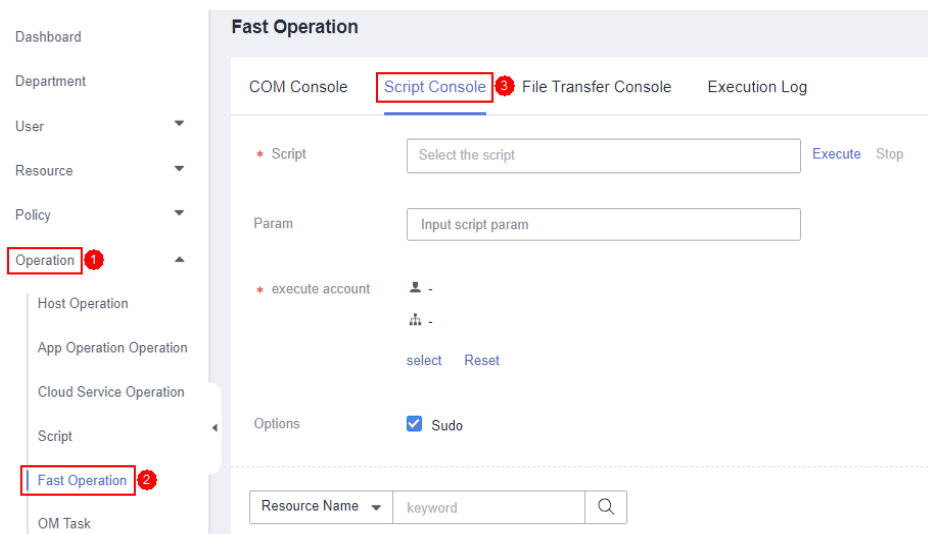
Step 4 Configure script O&M information. **Script O&M parameters** describes the parameters.
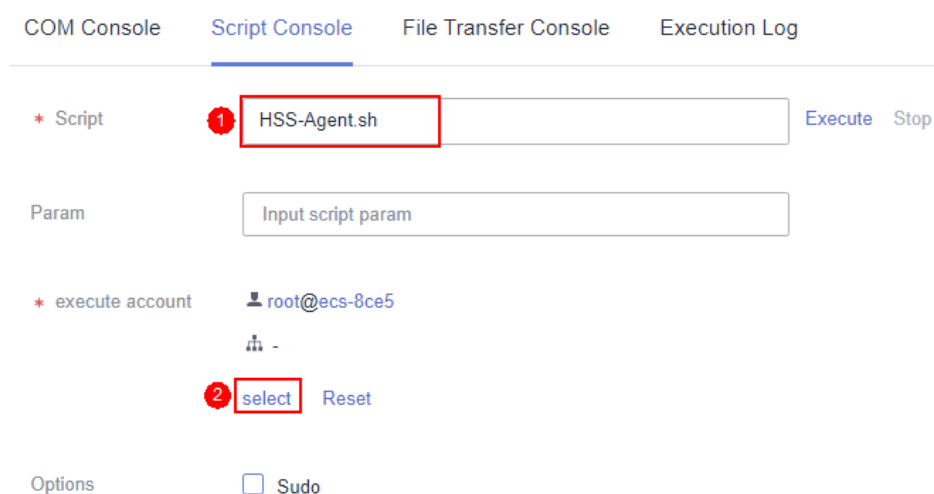
Figure 5-2 Configuring script O&M information

Table 5-1 Script O&M parameters

| Parameter	Description
Script	Select the **HSS-Agent.sh** script.
Param	Leave this parameter blank.
execute account	Click **select**, and select the account or account group of the server where the agent is to be installed.
Options	This parameter is optional. By default, the script task is executed in the Sudoers file on the server. If the server account does not have the execute permission on the file, select **Sudo**.

Step 5 Click **Execute**.

Figure 5-3 Executing a script task

Step 6 After the script task is successfully executed, click **Collapse** in the **Result** column to expand the execution result.

If **install finished.[OK]** is displayed, the agent is successfully installed.

**Figure 5-4** Successfully executed a script task
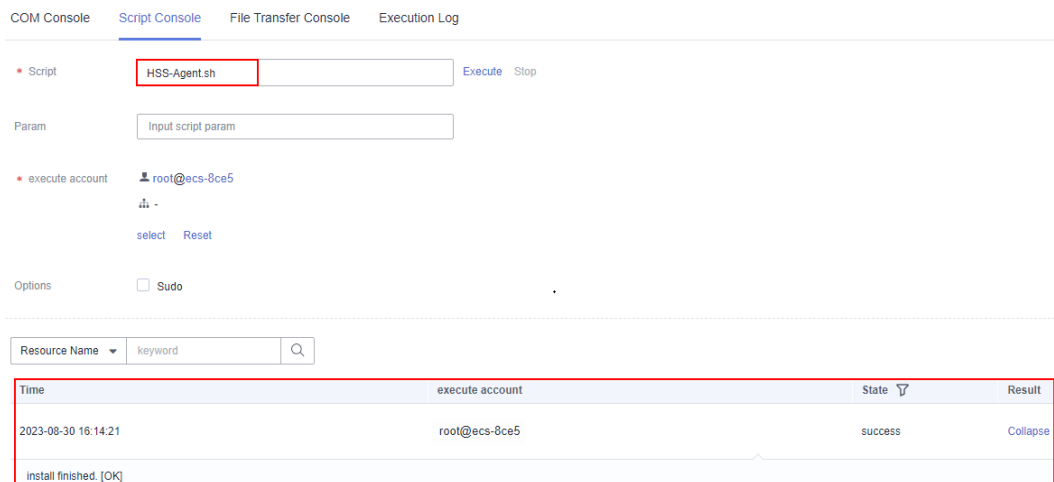
Step 7 On the Host Security Service console, confirm the agent installation result.

1. Log in to the Host Security Service console.

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

3. On the **Servers** tab page, check the agent status of the target server, as shown in **Checking the agent status**.

   If the agent status is **Online**, the agent is successfully installed.

   Figure 5-5 Checking the agent status
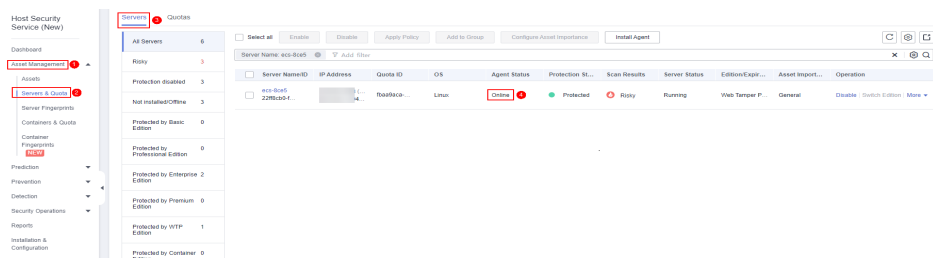
----End

A Change History

Released On	Description
2024-03-12	This issue is the third official release. Added: **HSS Multi-Cloud Management and Deployment** **Installing the Host Security Service Agent Using CBH**
2023-09-20	This issue is the second official release. Added: **Detecting and Fixing Vulnerabilities**
2023-08-08	This issue is the first official release.