## Host Security Service (HSS)

# Best Practices

**Issue** 10

**Date** 2025-01-07

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

## Trademarks and Permissions

## Notice

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

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

## Huawei Cloud Computing Technologies Co., Ltd.

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

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

# Contents

**1 HSS Best Practices You May Need........................................................................... 1**

**2 Suggestions on How to Fix Official Disclosed Vulnerabilities Provided by HSS...... 3**

2.1 Git Credential Disclosure Vulnerability (CVE-2020-5260)........................................3

2.2 SaltStack Remote Command Execution Vulnerabilities (CVE-2020-11651 and CVE-2020-11652)............5

2.3 OpenSSL High-risk Vulnerability (CVE-2020-1967)...................................................... 7

2.4 Adobe Font Manager Library Remote Code Execution Vulnerability (CVE-2020-1020/CVE-2020-0938) .................................................................................................................... 8

2.5 Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027)........................ 9

2.6 Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)...................................10

**3 Third-Party Servers Accessing HSS Through a Direct Connect and Proxy Servers .........................................................................................................13**

3.1 Overview.................................................................................................. 13

3.2 Resources and Costs...................................................................................14

3.3 Process Flow............................................................................................. 14

3.4 Process..................................................................................................... 15

3.4.1 Creating a Direct Connect.......................................................................... 15

3.4.2 Creating a Proxy Server............................................................................. 20

3.4.3 Installing an Agent on the Proxy Server.......................................................21

3.4.4 Installing and Configuring Nginx on the Proxy Server.................................. 23

3.4.5 Creating an Agent Installation Package or Installation Commands Using a Proxy Server......................27

3.4.6 Installing an Agent for a Third-Party Server.................................................. 30

**4 Connecting Third-Party Servers to HSS Through Direct Connect and VPC Endpoint .........................................................................................................32**

4.1 Overview.................................................................................................. 32

4.2 Resources and Costs...................................................................................33

4.3 Process Flow............................................................................................. 34

4.4 Process..................................................................................................... 34

4.4.1 Creating a Direct Connect.......................................................................... 34

4.4.2 Creating a VPC Endpoint.............................................................................40

4.4.3 Obtaining a Project ID................................................................................ 40

4.4.4 Generating the Agent Installation Package or Installation Command................41

4.4.5 Installing an Agent for a Third-Party Server.................................................. 44

**5 Installing the HSS Agent Using CBH.......... 46**

**6 Using HSS to Improve Server Login Security.......... 49**

**7 Using HSS and CBR to Defend Against Ransomware.......... 60**

7.1 Overview.......... 60

7.2 Resources and Costs.......... 63

7.3 Defense Measures.......... 63

7.3.1 Identifying and Fixing Ransomware.......... 63

7.3.2 Enabling Ransomware Prevention and Backup.......... 66

7.3.3 Restoring Backup Data.......... 73

**8 Using HSS to Scan and Fix Vulnerabilities.......... 75**

**9 Using HSS to Prevent Weak Passwords.......... 81**

**10 Using HSS to Scan for Trojans.......... 86**

**11 Using HSS to Handle Mining Attacks.......... 88**

**12 Using HSS to Monitor the Integrity of Linux Server Files.......... 94**

**13 Whitelist Can Be Used to Avoid False Alarm Reporting.......... 103**

# 1 HSS Best Practices You May Need

This document summarizes the operation practices of Host Security Service (HSS) in common application scenarios. It provides explicit solution descriptions and operation guidance for each scenario, making it easier for you to use HSS to improve the security of servers and containers.

## HSS Best Practices

**Table 1-1** Best practices

| Category | Related Document |
|---|---|
| Access HSS | **Connecting Third-Party Servers to HSS Through Direct Connect and VPC Endpoint** |
| | **Third-Party Servers Accessing HSS Through a Direct Connect and Proxy Servers** |
| | **Installing the HSS Agent Using CBH** |
| Server login protection | **Using HSS to Improve Server Login Security** |
| Vulnerability fixing | **Git Credential Disclosure Vulnerability (CVE-2020-5260)** |
| | **SaltStack Remote Command Execution Vulnerabilities (CVE-2020-11651 and CVE-2020-11652)** |
| | **OpenSSL High-risk Vulnerability (CVE-2020-1967)** |
| | **Adobe Font Manager Library Remote Code Execution Vulnerability (CVE-2020-1020/CVE-2020-0938)** |
| | **Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027)** |
| | **Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)** |
| | **Using HSS to Scan and Fix Vulnerabilities** |

| Category | Related Document |
|---|---|
| Weak password protection | **Using HSS to Prevent Weak Passwords** |
| Ransomware prevention | **Using HSS and CBR to Defend Against Ransomware** |
| Intrusion detection | **Using HSS to Scan for Trojans** |
| | **Using HSS to Handle Mining Attacks** |
| | **Whitelist Can Be Used to Avoid False Alarm Reporting** |
| File protection | **Using HSS to Monitor the Integrity of Linux Server Files** |

# 2 Suggestions on How to Fix Official Disclosed Vulnerabilities Provided by HSS

## 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.

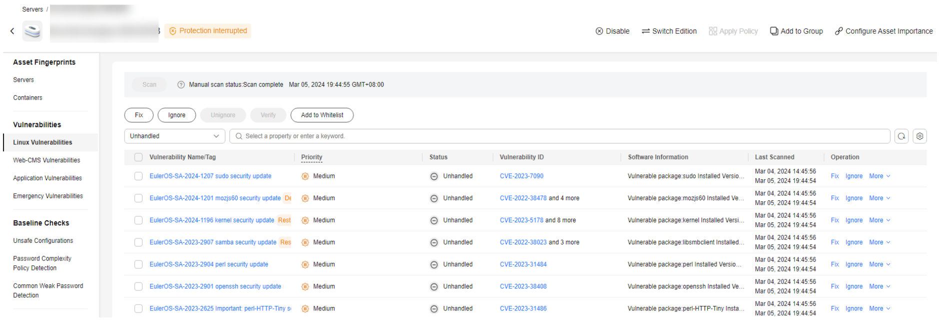
Download address: **https://github.com/git/git/releases**

## Suggestion

Perform the following steps to scan and fix a vulnerability.

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

**Figure 2-1** Manually starting a vulnerability scan



Manual scan status:Scan complete Mar 05, 2024 19:44:55 GMT+08:00

| Vulnerability Name/Tag | Priority | Status | Vulnerability ID | Software Information | Last Scanned | Operation |
|---|---|---|---|---|---|---|
| EulerOS-SA-2024-1207 sudo security update | Medium | Unhandled | CVE-2023-7090 | Vulnerable package:sudo Installed Versio... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| EulerOS-SA-2024-1201 mozjs60 security update De | Medium | Unhandled | CVE-2022-38478 and 4 more | Vulnerable package:mozjs60 Installed Ve... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| EulerOS-SA-2024-1196 kernel security update Rest | Medium | Unhandled | CVE-2023-5178 and 8 more | Vulnerable package:kernel Installed Versi... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| EulerOS-SA-2023-2907 samba security update Res | Medium | Unhandled | CVE-2022-38023 and 3 more | Vulnerable package:libsmbclient Installed... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| EulerOS-SA-2023-2904 perl security update | Medium | Unhandled | CVE-2023-31484 | Vulnerable package:perl Installed Versio... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| EulerOS-SA-2023-2901 openssh security update | Medium | Unhandled | CVE-2023-38408 | Vulnerable package:openssh Installed Ve... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| EulerOS-SA-2023-2625 Important: perl-HTTP-Tiny s | Medium | Unhandled | CVE-2023-31486 | Vulnerable package:perl-HTTP-Tiny Insta... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |

**Step 2** Fix and verify the vulnerability. For details about the operation procedure, see **Fixing Vulnerabilities and Verifying the Result**.

**----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.

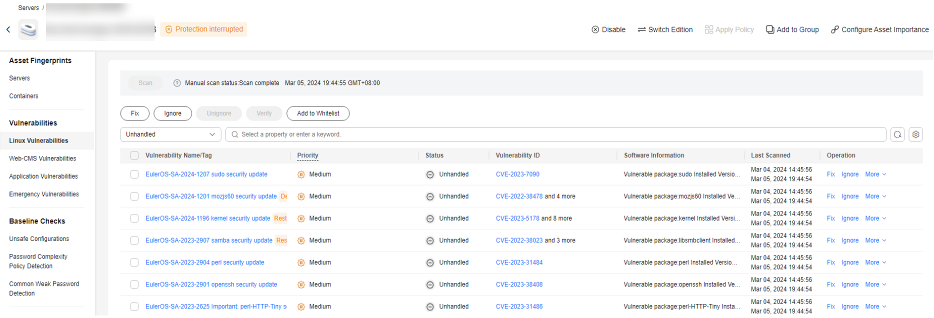
## Suggestion

Perform the following steps to scan and fix a vulnerability.

- Scan and view details of a vulnerability. For details, see **Viewing Details of a Vulnerability**.

  Fix and verify the vulnerability. For details about the operation procedure, see **Fixing Vulnerabilities and Verifying the Result**.

  **Figure 2-2** Manually starting a vulnerability scan

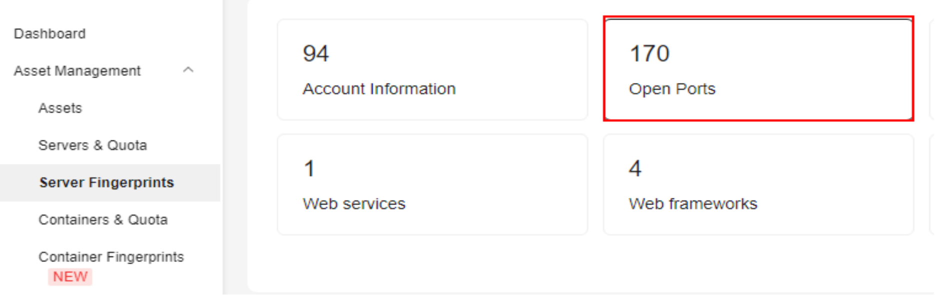
  Manual scan status:Scan complete Mar 05, 2024 19:44:55 GMT+08:00

  | | Vulnerability Name/Tag | Priority | Status | Vulnerability ID | Software Information | Last Scanned | Operation |
  |---|---|---|---|---|---|---|---|
  | □ | EulerOS-SA-2024-1207 sudo security update | Medium | Unhandled | CVE-2023-7090 | Vulnerable package:sudo Installed Versio... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
  | □ | EulerOS-SA-2024-1201 mozjs60 security update De | Medium | Unhandled | CVE-2022-38478 and 4 more | Vulnerable package:mozjs60 Installed Ve... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
  | □ | EulerOS-SA-2024-1196 kernel security update Rest | Medium | Unhandled | CVE-2023-5178 and 8 more | Vulnerable package:kernel Installed Versi... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
  | □ | EulerOS-SA-2023-2907 samba security update Res | Medium | Unhandled | CVE-2022-38023 and 3 more | Vulnerable package:libsmbclient Installed... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
  | □ | EulerOS-SA-2023-2904 perl security update | Medium | Unhandled | CVE-2023-31484 | Vulnerable package:perl Installed Versio... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
  | □ | EulerOS-SA-2023-2901 openssh security update | Medium | Unhandled | CVE-2023-38408 | Vulnerable package:openssh Installed Ve... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
  | □ | EulerOS-SA-2023-2625 Important: perl-HTTP-Tiny s | Medium | Unhandled | CVE-2023-31486 | Vulnerable package:perl-HTTP-Tiny Insta... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |

- 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. For details, see **Checking Open Ports**

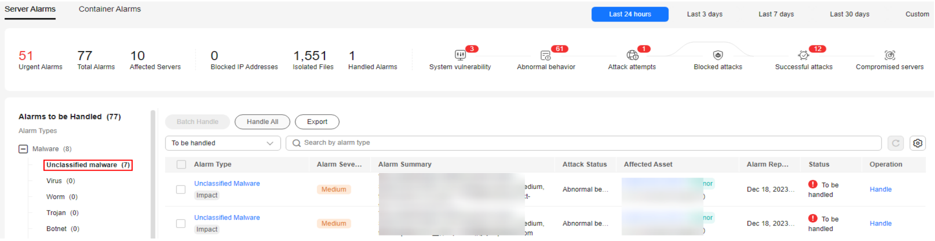
  **Figure 2-3** Server fingerprints

- Check for, isolate, and kill Trojans.

  Isolate and kill the mining Trojans. For details, see **Isolation and Killing**..

**Figure 2-4** Managing the isolated files



| □ | Alarm Type | Alarm Seve... | Alarm Summary | Attack Status | Affected Asset | Alarm Rep... | Status | Operation |
|---|---|---|---|---|---|---|---|---|
| □ | Unclassified Malware<br>Impact | Medium | [redacted] | Abnormal be... | [redacted] | Dec 18, 2023... | To be handled | Handle |
| □ | Unclassified Malware<br>Impact | Medium | [redacted] | Abnormal be... | [redacted] | Dec 18, 2023... | To be handled | Handle |

# 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.

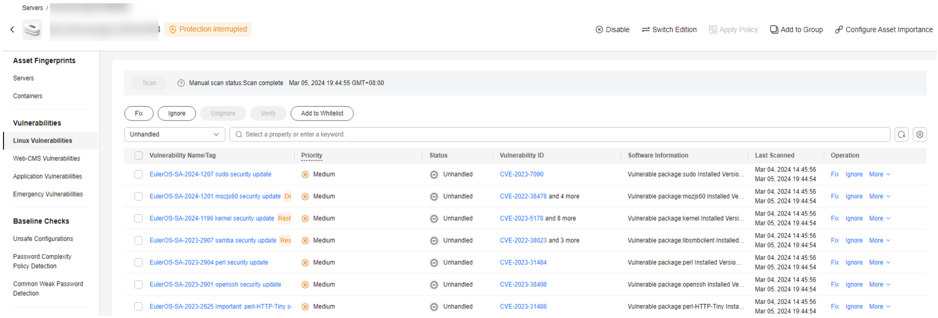
- **https://www.debian.org/security/2020/dsa-4661**
- **https://security.gentoo.org/glsa/202004-10**
- **https://lists.suse.com/pipermail/sle-security-updates/2020-April/006722.html**

## 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 2-5** Manually starting a vulnerability scan



Manual scan status:Scan complete Mar 05, 2024 19:44:55 GMT+08:00

Unhandled

| | Vulnerability Name/Tag | Priority | Status | Vulnerability ID | Software Information | Last Scanned | Operation |
|---|---|---|---|---|---|---|---|
| □ | EulerOS-SA-2024-1207 sudo security update | Medium | Unhandled | CVE-2023-7090 | Vulnerable package:sudo Installed Versio... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| □ | EulerOS-SA-2024-1201 mozjs60 security update De | Medium | Unhandled | CVE-2022-38478 and 4 more | Vulnerable package:mozjs60 Installed Ve... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| □ | EulerOS-SA-2024-1196 kernel security update Rest | Medium | Unhandled | CVE-2023-5178 and 8 more | Vulnerable package:kernel Installed Versi... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| □ | EulerOS-SA-2023-2907 samba security update Res | Medium | Unhandled | CVE-2022-38023 and 3 more | Vulnerable package:libsmbclient Installed... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| □ | EulerOS-SA-2023-2904 perl security update | Medium | Unhandled | CVE-2023-31484 | Vulnerable package:perl Installed Versio... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| □ | EulerOS-SA-2023-2901 openssh security update | Medium | Unhandled | CVE-2023-38408 | Vulnerable package:openssh Installed Ve... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |
| □ | EulerOS-SA-2023-2625 Important: perl-HTTP-Tiny s | Medium | Unhandled | CVE-2023-31486 | Vulnerable package:perl-HTTP-Tiny Insta... | Mar 04, 2024 14:45:56<br>Mar 05, 2024 19:44:54 | Fix Ignore More |

**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.

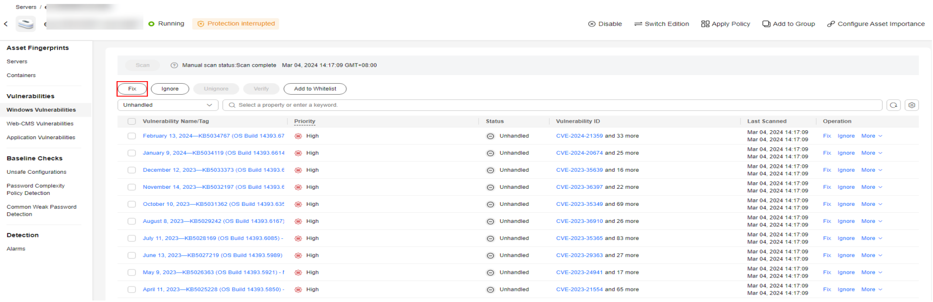
For details, see https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1020.

## Suggestion

Perform the following steps to scan and fix a vulnerability.

**Step 1** Scan and view details of a vulnerability. For details, see **Viewing Details of a Vulnerability**.

**Figure 2-6** Manually starting a vulnerability scan



Manual scan status:Scan complete Mar 04, 2024 14:17:09 GMT+08:00

| Vulnerability Name/Tag | Priority | Status | Vulnerability ID | Last Scanned | Operation |
|---|---|---|---|---|---|
| February 13, 2024—KB5034767 (OS Build 14393.67 | High | Unhandled | CVE-2024-21359 and 33 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| January 9, 2024—KB5034119 (OS Build 14393.6614 | High | Unhandled | CVE-2024-20674 and 25 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| December 12, 2023—KB5033373 (OS Build 14393.6 | High | Unhandled | CVE-2023-35639 and 16 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| November 14, 2023—KB5032197 (OS Build 14393.6 | High | Unhandled | CVE-2023-36397 and 22 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| October 10, 2023—KB5031362 (OS Build 14393.635 | High | Unhandled | CVE-2023-35349 and 69 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| August 8, 2023—KB5029242 (OS Build 14393.6167) | High | Unhandled | CVE-2023-36910 and 26 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| July 11, 2023—KB5028169 (OS Build 14393.6085) - | High | Unhandled | CVE-2023-35365 and 83 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| June 13, 2023—KB5027219 (OS Build 14393.5989) | High | Unhandled | CVE-2023-29363 and 27 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| May 9, 2023—KB5026363 (OS Build 14393.5921) - I | High | Unhandled | CVE-2023-24941 and 17 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| April 11, 2023—KB5025228 (OS Build 14393.5850) - | High | Unhandled | CVE-2023-21554 and 65 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |

**Step 2** Fix and verify the vulnerability. For details about the operation procedure, see **Fixing Vulnerabilities and Verifying the Result**.

**----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.

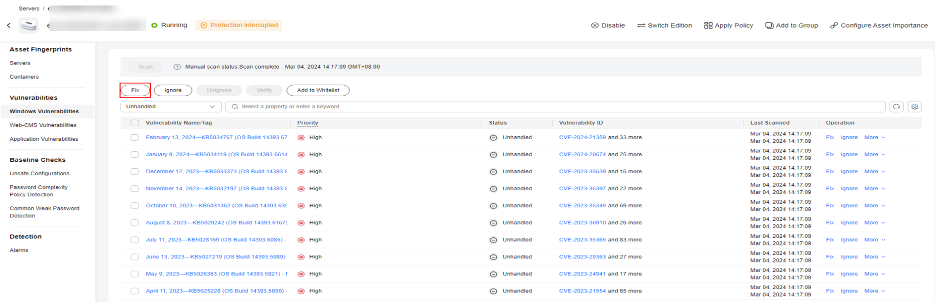
For details, see https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1027.

## 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 2-7** Manually starting a vulnerability scan



Manual scan status:Scan complete Mar 04, 2024 14:17:09 GMT+08:00

| Vulnerability Name/Tag | Priority | Status | Vulnerability ID | Last Scanned | Operation |
|---|---|---|---|---|---|
| February 13, 2024—KB5034767 (OS Build 14393.67 | High | Unhandled | CVE-2024-21359 and 33 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| January 9, 2024—KB5034119 (OS Build 14393.6614 | High | Unhandled | CVE-2024-20674 and 25 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| December 12, 2023—KB5033373 (OS Build 14393.6 | High | Unhandled | CVE-2023-35639 and 16 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| November 14, 2023—KB5032197 (OS Build 14393.6 | High | Unhandled | CVE-2023-36397 and 22 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| October 10, 2023—KB5031362 (OS Build 14393.635 | High | Unhandled | CVE-2023-35349 and 69 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| August 8, 2023—KB5029242 (OS Build 14393.6167) | High | Unhandled | CVE-2023-36910 and 26 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| July 11, 2023—KB5028169 (OS Build 14393.6085) - | High | Unhandled | CVE-2023-35365 and 83 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| June 13, 2023—KB5027219 (OS Build 14393.5989) | High | Unhandled | CVE-2023-29363 and 27 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| May 9, 2023—KB5026363 (OS Build 14393.5921) - I | High | Unhandled | CVE-2023-24941 and 17 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| April 11, 2023—KB5025228 (OS Build 14393.5850) - | High | Unhandled | CVE-2023-21554 and 65 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |

**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 HSS agent on the server to be fixed, and has enabled protection.

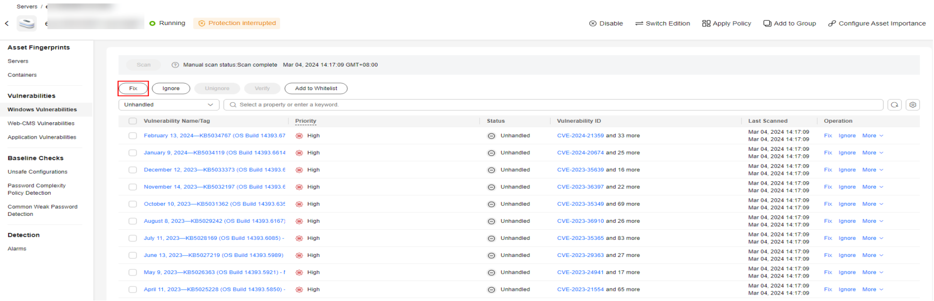
**Step 1** Log in to the management console.

**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security and Compliance** > HSS. The HSS 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 2-8** Manually starting a vulnerability scan



Manual scan status:Scan complete Mar 04, 2024 14:17:09 GMT+08:00

| □ | Vulnerability Name/Tag | Priority | Status | Vulnerability ID | Last Scanned | Operation |
|---|---|---|---|---|---|---|
| □ | February 13, 2024—KB5034767 (OS Build 14393.67 | High | Unhandled | CVE-2024-21359 and 33 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| □ | January 9, 2024—KB5034119 (OS Build 14393.6614 | High | Unhandled | CVE-2024-20674 and 25 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| □ | December 12, 2023—KB5033373 (OS Build 14393.6 | High | Unhandled | CVE-2023-35639 and 16 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| □ | November 14, 2023—KB5032197 (OS Build 14393.6 | High | Unhandled | CVE-2023-36397 and 22 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| □ | October 10, 2023—KB5031362 (OS Build 14393.635 | High | Unhandled | CVE-2023-35349 and 69 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| □ | August 8, 2023—KB5029242 (OS Build 14393.6167) | High | Unhandled | CVE-2023-36910 and 26 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| □ | July 11, 2023—KB5028169 (OS Build 14393.6085) - | High | Unhandled | CVE-2023-35365 and 83 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| □ | June 13, 2023—KB5027219 (OS Build 14393.5989) | High | Unhandled | CVE-2023-29363 and 27 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| □ | May 9, 2023—KB5026363 (OS Build 14393.5921) - I | High | Unhandled | CVE-2023-24941 and 17 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |
| □ | April 11, 2023—KB5025228 (OS Build 14393.5850) - | High | Unhandled | CVE-2023-21554 and 65 more | Mar 04, 2024 14:17:09<br>Mar 04, 2024 14:17:09 | Fix Ignore More |

**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 Third-Party Servers Accessing HSS Through a Direct Connect and Proxy Servers

## 3.1 Overview

### Scenario

With the development of hybrid clouds, there is also a growing need for companies to perform unified security management of on- and off-cloud or hybrid clouds. HSS supports the access and management of third-party cloud servers and on-premises IDCs. Users are allowed to use the same security policies on different clouds, preventing the risks caused by inconsistent security policies.

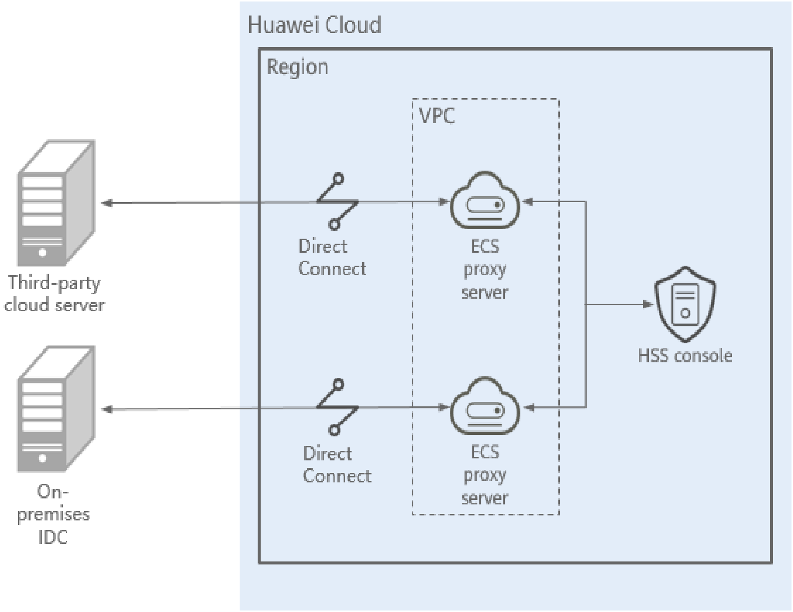
For third-party cloud servers and on-premises IDCs that cannot access the public network, you can refer to this solution to access HSS through **Direct Connect and a proxy** for protection management. If your server can access the Internet, connect the server to HSS by referring to **Installing the Agent for a Third-Party Server**.

### Architecture

Third-party servers communicate with VPCs on the cloud through Direct Connect, and then connect to HSS through ECS agent, as shown in **Connecting a third-party server to HSS through Direct Connect and ECS agent**.

- **Direct Connect** establishes a dedicated network connection that features high speed, low latency, stability, and security between your on-premises data center and Huawei Cloud VPC. Direct Connect allows you to maximize legacy IT facilities and leverage cloud services to build a flexible, scalable hybrid cloud compute environment.
- **Elastic Cloud Server (ECS)** is a scalable and on-demand cloud server. It helps you to efficiently set up reliable, secure, and flexible application environments, ensuring stable service running and improving O&M efficiency.

**Figure 3-1** A third-party server accessing HSS through a Direct Connect and proxy servers



## Advantages

This solution has no restrictions on regions. The third-party server can access any region.

# 3.2 Resources and Costs

The following table lists resources in this example.

**Table 3-1** Resource description

| Resource | Description | Quantity | Cost |
|---|---|---|---|
| Direct Connect | Direct Connect is used to connect third-party servers and cloud resources. | 2 | For details, see **DC Pricing Details**. |
| Elastic Cloud Server (ECS) | ECS, as a proxy server, forwards requests from third party servers to the HSS. | 2 | For details, see **ECS Pricing Details**. |

# 3.3 Process Flow

The process for third-party cloud servers and on-premises IDC to access HSS through Direct Connect and proxy servers is as follows:

1. **Creating a Direct Connect**

   If a third-party server cannot access the public network, you need to create a Direct Connect to connect to the VPC on the cloud for network interconnection.

2. **Creating a Proxy Server**

   You need to create a third-party server as the proxy server to connect to the third-party server.

3. **Installing an Agent on the Proxy Server**

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

4. **Installing and Configuring Nginx on the Proxy Server**

   Nginx forwards requests from a third-party server to the HSS management console.

5. **Creating an Agent Installation Package or Installation Commands Using a Proxy Server**

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

6. **Installing the Agent for a Third-Party Server**

   Install an agent for a third-party server and connect the server to HSS for unified management.

# 3.4 Process

## 3.4.1 Creating a Direct Connect

Third-party servers and on-premises IDCs can use Direct Connect to access servers in VPCs on the cloud without using the public network.

For details about Direct Connect, see **Direct Connect Introduction**.

### Creating a Direct Connect

For details, see **Using Direct Connect to Connect an On-Premises Data Center to the Cloud**.

**Step 1** Create a connection.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the region and project.
3. Click ☰ in the upper left corner of the page and choose **Networking** > **Direct Connect** to switch to the **Connections** page.
4. Click **Create Connection**.
5. On the **Create Connection** page, enter the equipment room details and select the Direct Connect location and port based on **Table 3-2**.

**Table 3-2** Parameters required for creating a cloud connection

| Parameter | Description |
|---|---|
| Billing Mode | Specifies how you are charged. Currently, only **Yearly/Monthly** is supported. |
| Region | Specifies the region where the connection is deployed. You can change the region in the upper left corner of the console. |
| Connection Name | Specifies the name of your connection. |
| Location | Specifies the location where your leased line can connect to. |
| Carrier | Specifies the carrier that provides the leased line. |
| Port Type | Specifies the type of the port used by the connection. There are four types of ports: 1GE, 10GE, 40GE, and 100GE. |
| Leased Line Bandwidth | Specifies the bandwidth of the leased line in the unit of Mbit/s. This is the bandwidth of the leased line you bought from the carrier. |
| Your Equipment Room Address | Specifies the address of your equipment room. The address must be specific to the floor your equipment room is on, |
| Tag | Identifies the connection. A tag consists of a key and a value. You can add 10 tags to a connection.<br>**NOTE**<br>If a predefined tag has been created in TMS, you can select the corresponding tag key and value.<br>For details about predefined tags, see **Predefined Tag Overview**. |
| Description | Provides supplementary information about the connection. |

| Parameter | Description |
|---|---|
| Contact Person/Phone Number/ Email | Specifies information about the person who is responsible for your connection.<br>If no contact information is provided, we will contact the person in your account information. This will prolong the review period. |
| Required Duration | Specifies how long the connection will be used for. |
| Auto-renewing DBSS | Specifies whether to automatically renew the connection to ensure service continuity.<br>It is recommended that you set the auto-renewal period to be the same as the required duration. If the required duration is three months, the system automatically renews the subscription for every three months. |
| Enterprise Project | Specifies an enterprise project by which cloud resources and members are centrally managed. |

6. Click **Confirm Configuration**.
7. Confirm the configuration and click **Request Connection**.

   Confirm the requirements with the Direct Connect manager.
8. After the system approves the requirement, the user needs to contact the carrier for construction.

   After the construction is complete, locate the connection in the connection list and click **Confirm Cabling** in the **Operation** column.
9. In the displayed dialog box, click **OK**.
10. In the connection list, locate the connection and click **Confirm Configuration** in the **Operation** column.
11. Confirm the configuration and click **Pay Now**.
12. Confirm the order, select a payment method, and click **Confirm**.
13. After the payment is complete, wait for Huawei Cloud to complete the construction.

    Huawei onsite engineers will connect the Direct Connect connection to the Huawei Cloud gateway port based on the customer information within two working days.
14. Verify that the connection is in the **Normal** state, which means that the connection is ready, and the billing starts.

**Step 2** Create a virtual gateway.

1. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**.
2. In the upper right corner of the **Virtual Gateways** page, click **Create Virtual Gateway**.
3. Configure the virtual gateway parameters.

**Table 3-3** Virtual gateway parameters

| Parameter | Description |
|---|---|
| Name | Specifies the virtual gateway name.<br>You can enter 1 to 64 characters. |
| Enterprise Project | Specifies the enterprise project by which virtual gateways are centrally managed. Select an existing enterprise project. |
| VPC | Specifies the VPC to be associated with the virtual gateway. |
| Subnet CIDR Block | Specifies CIDR blocks of the VPC subnets.<br>You can enter one or more CIDR blocks and separate every entry with a comma (,). |
| BGP ASN | Specifies the BGP ASN of the virtual gateway. |
| Tag | Adds tags to help you identify your virtual gateway. You can change them after the virtual gateway is created. |
| Description | Provides supplementary information about the virtual gateway. |

4. Click **OK**.

**Step 3** Create a virtual interface.

1. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.
2. Click **Create Virtual Interface**.
3. Configure the parameters as prompted.

**Table 3-4** Parameters for creating a virtual interface

| Parameter | Description |
|---|---|
| Region | Specifies the region where the connection is deployed. You can change the region in the upper left corner of the console. |
| Name | Specifies the virtual interface name.<br>The name can contain 1 to 64 characters. |

| Parameter | Description |
|---|---|
| Virtual Interface Priority | Specifies whether the virtual interface will be used prior to other virtual interfaces. There are two options: **Preferred** and **Standard**.<br>If multiple virtual interfaces are associated with one Direct Connect device, the load is balanced among virtual interfaces with the same priority, while virtual interfaces with different priorities are working in active/standby pairs. |
| Connection | Specifies the connection you use to connect your data center to the cloud. |
| Gateway | Specifies the gateway that the virtual interface connects to.<br>You can select a virtual gateway or global DC gateway. |
| Virtual Gateway | This parameter is mandatory when **Gateway** is set to **Virtual gateway**.<br>Specifies the virtual gateway that the virtual interface connects to. |
| Global DC Gateway | This parameter is mandatory when **Gateway** is set to **Global DC gateway**.<br>Specifies the global DC gateway that the virtual interface connects to. |
| VLAN | Specifies the ID of the VLAN for the virtual interface.<br>You need to configure the VLAN if you create a standard connection.<br>The VLAN for a hosted connection will be allocated by the carrier or partner. You do not need to configure the VLAN. |
| Bandwidth | Specifies the bandwidth that can be used by the virtual interface in the unit of Mbit/s. The bandwidth cannot exceed that of the connection. |
| Enterprise Project | Specifies the enterprise project by which virtual interfaces are centrally managed. Select an existing enterprise project. |
| Tag | Adds tags to help you identify your virtual interface. You can change them after the virtual interface is created. |
| Local Gateway | Specifies the IP address used by the cloud to connect to your on-premises network. After you configure **Local Gateway** on the console, the configuration will be automatically delivered to the gateway used by the cloud. |

| Parameter | Description |
|---|---|
| Remote Gateway | Specifies the IP address used by the on-premises data center to connect to the cloud. After you configure **Remote Gateway** on the console, you need to configure the IP address on the interface of the on-premises device. |
| Remote Subnet | Specifies the subnets of your on-premises network. Separate every entry with a comma (.). |
| Routing Mode | Specifies the routing mode. Two options are available, **Static** and **BGP**.<br>If there are two or more connections, select BGP routing. |
| BGP ASN | Specifies the ASN of the BGP peer.<br>This parameter is mandatory when you select BGP routing. |
| BGP MD5 Authentication Key | Specifies the password used to authenticate the BGP peer using MD5.<br>This parameter can be set when BGP routing is selected, and the parameter values on both gateways must be the same.<br>The key contains 8 to 255 characters and must contain at least two types of the following characters:<br>– Uppercase letter<br>– Lowercase letter<br>– Digits<br>– Special characters ~!, .:;-_"(){}[]/@#$ %^&*+\&#124;= |
| Description | Provides supplementary information about the virtual interface. |

4. Click **Create Now**.

   When the status changes to **Normal**, the virtual interface has been created.

**Step 4** Configure local routes on the on-premises data centers.

After your on-premises network is connected to Huawei Cloud, you need to configure routes in your data center.

- For details about how to configure static routes, see **Accessing a VPC Using a Static Routing Connection**.
- For details about how to configure BGP routes, see **Accessing a VPC Using a BGP Routing Connection**.

**----End**

## 3.4.2 Creating a Proxy Server

Create a server on the cloud to function as a proxy server of the third-party server.

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.
- The image of the proxy server must be a Linux image that can use the **yum** command. You are advised to use the HCE image.

## Creating a Proxy Server

**Step 1** Log in to the console and choose **Buy an ECS**.

**Step 2** On the page for purchasing the ECS, set the parameters.

- CPU Architecture: In this example, select **x86**.
- Specifications: In this example, select **c6.xlarge.2**.
- Image: In this example, select **Public image Huawei Cloud EulerOS 2.0 Standard 64 bit (40 GiB)**.
- Other parameters: Set the parameters as prompted based on the site requirements.

**Step 3** Confirm all information, click **Create**. In the displayed dialog box, click **Agree and Create**. After the payment is complete, the ECS is automatically created and started by default.

**----End**

# 3.4.3 Installing an Agent on the Proxy Server

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

## Installing an Agent on the Proxy Server

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

**Step 2** Click 📍 in the upper left corner and select the region and project.

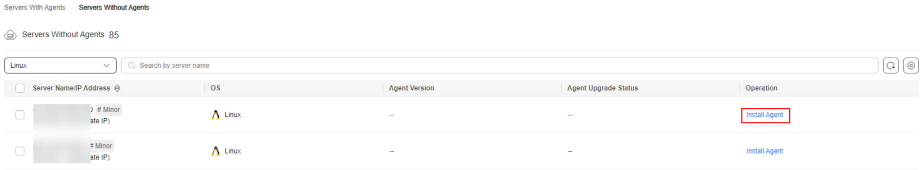
**Step 3** Click ☰ in the upper left corner of the page and choose **Security & Compliance** > HSS.

**Step 4** In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

**Step 5** Choose **Agents** > **Servers Without Agents**.

**Step 6** In the **Operation** column of the target server, click **Install Agent**. The **Install Agent** dialog box is displayed.

**Figure 3-2** Installing an agent



Servers With Agents | Servers Without Agents

Servers Without Agents 85

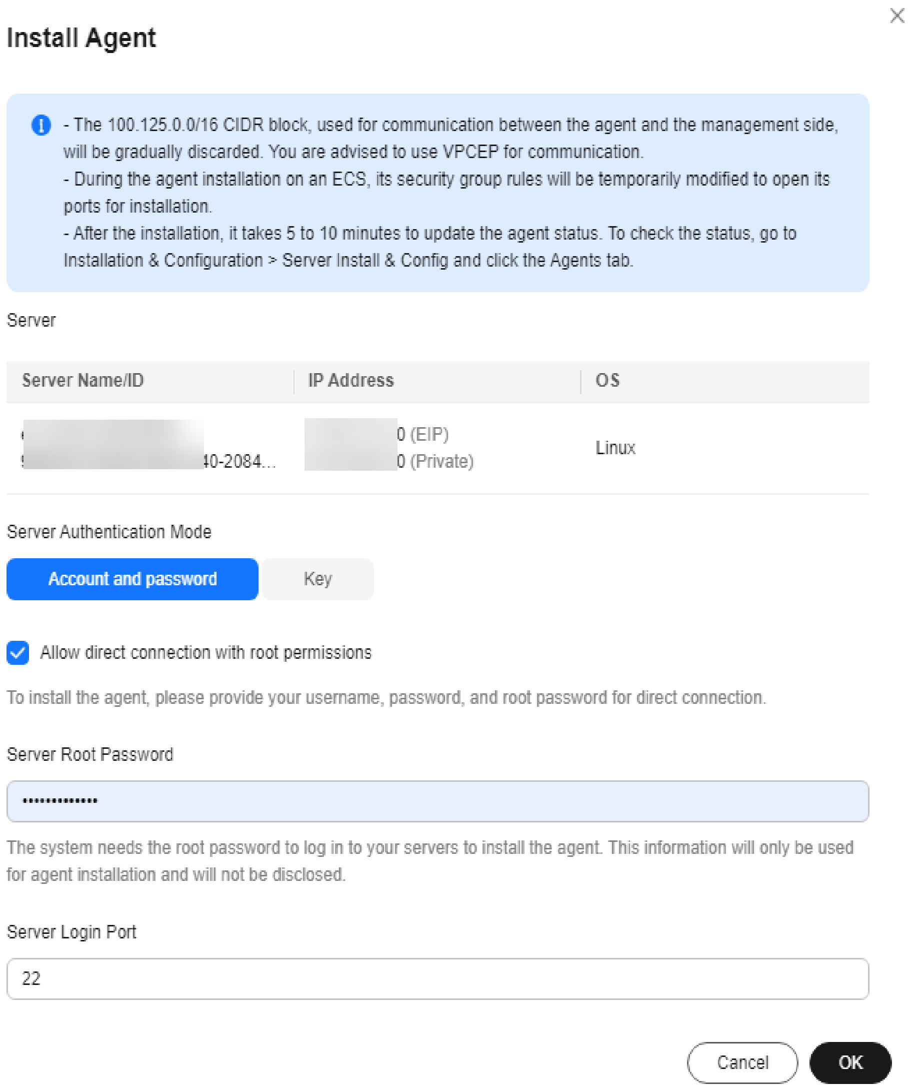
Linux | Search by server name

| ☐ Server Name/IP Address | OS | Agent Version | Agent Upgrade Status | Operation |
|---|---|---|---|---|
| ☐ [redacted] # Minor ate IP) | Linux | -- | -- | Install Agent |
| ☐ [redacted] # Minor ate IP) | Linux | -- | -- | Install Agent |

**Step 7** Select and set the server verification information.

- **Server authentication mode**: Select a mode. In this example, select **Account and password** mode.
- Allow direct connection as user **root**: Depends on whether the server allows direct connection as user **root**. In this example, select this option.
  - **Server Root Password**: Set this parameter based on the server information.
  - **Server Login Port**: Set this parameter based on the actual server login port. In this example, set **22** port.

**Figure 3-3** Enter the server verification information.



Install Agent

- The 100.125.0.0/16 CIDR block, used for communication between the agent and the management side, will be gradually discarded. You are advised to use VPCEP for communication.
- During the agent installation on an ECS, its security group rules will be temporarily modified to open its ports for installation.
- After the installation, it takes 5 to 10 minutes to update the agent status. To check the status, go to Installation & Configuration > Server Install & Config and click the Agents tab.

Server

| Server Name/ID | IP Address | OS |
|---|---|---|
| [redacted] | [redacted] (EIP)<br>[redacted] (Private) | Linux |

Server Authentication Mode

**Account and password** | Key

☑ Allow direct connection with root permissions

To install the agent, please provide your username, password, and root password for direct connection.

Server Root Password

•••••••••••••

The system needs the root password to log in to your servers to install the agent. This information will only be used for agent installation and will not be disclosed.

Server Login Port

22

**Step 8** Click **OK** to start installation.

**Step 9** Choose **Servers With Agents** page and view the agent status of the target server.

If the **Agent Status** is **Online**, the agent is successfully installed.

**----End**

# 3.4.4 Installing and Configuring Nginx on the Proxy Server

Nginx forwards requests from a third-party server to the HSS management console.

## Installing and Configuring Nginx on the Proxy Server

**Step 1** Log in to the proxy server.

**Step 2** Check the Yum repository.

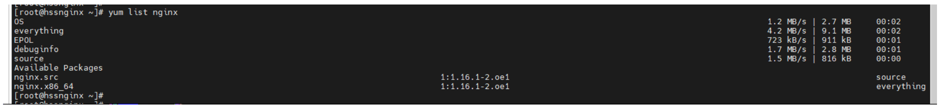
Check whether the Nginx software package exists in the Yum repository. If the Nginx software package does not exist, configure the Yum repository and bind the public IP address temporarily. After the installation is complete, unbind the public IP address.

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

- For EulerOS, CentOS and Red Hat, or other OSs that support RPM installation, run the **yum list nginx** command.
- For OSs that support DEB installation, such as Ubuntu and Debian, run the **apt list nginx** command.

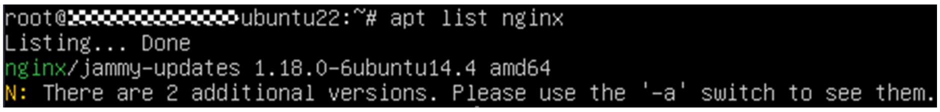
If the information shown in **The Nginx package exists (rpm)** or **The Nginx package exists (deb)** is displayed, the Nginx package exists.

**Figure 3-4** The Nginx package exists (rpm)



```
[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 ~]#
```

**Figure 3-5** The Nginx package exists (deb)

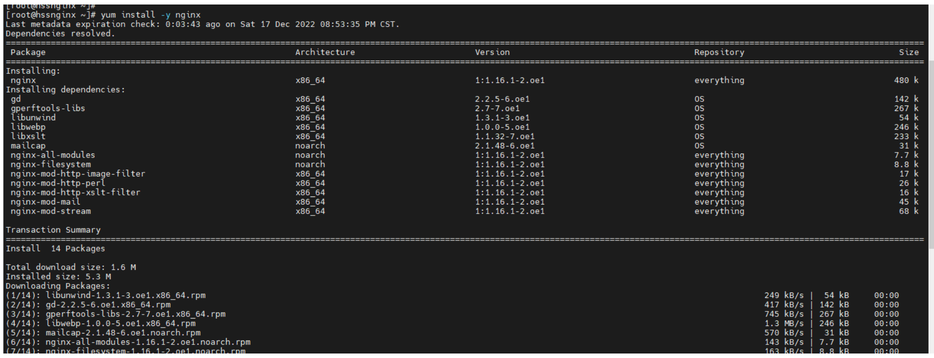


```
root@[redacted]ubuntu22:~# apt list nginx
Listing... Done
nginx/jammy-updates 1.18.0-6ubuntu14.4 amd64
N: There are 2 additional versions. Please use the '-a' switch to see them.
```

**Step 3** Installing Nginx

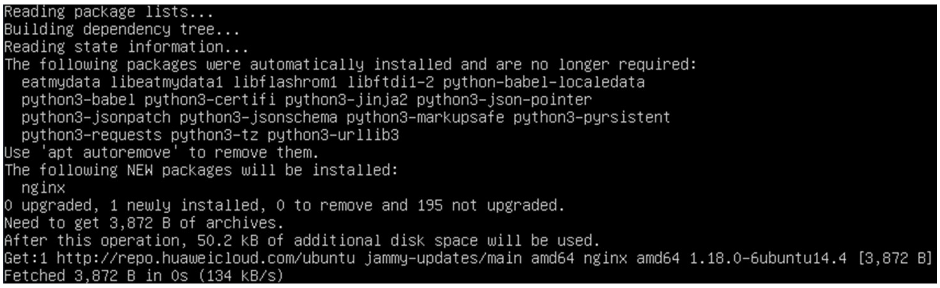
1. Run the following command to install Nginx using Yum:
   - For EulerOS, CentOS and Red Hat, or other OSs that support RPM installation, run the **yum install -y nginx** command.
   - For OSs that support DEB installation, such as Ubuntu and Debian, run the **apt install –y nginx** command.

**Figure 3-6** Installing Nginx (yum)



```
[root@hssnginx ~]#
[root@hssnginx ~]# yum install -y nginx
Last metadata expiration check: 0:03:43 ago on Sat 17 Dec 2022 08:53:35 PM CST.
Dependencies resolved.
==========================================================================================================================================================
 Package                             Architecture           Version                         Repository                                            Size
==========================================================================================================================================================
Installing:
 nginx                               x86_64                 1:1.16.1-2.oe1                  everything                                           480 k
Installing dependencies:
 gd                                  x86_64                 2.2.5-6.oe1                     OS                                                   142 k
 gperftools-libs                     x86_64                 2.7-7.oe1                       OS                                                   267 k
 libunwind                           x86_64                 1.3.1-3.oe1                     OS                                                    54 k
 libwebp                             x86_64                 1.0.0-5.oe1                     OS                                                   246 k
 libxslt                             x86_64                 1.1.32-7.oe1                    OS                                                   233 k
 mailcap                             noarch                 2.1.48-6.oe1                    OS                                                    31 k
 nginx-all-modules                   noarch                 1:1.16.1-2.oe1                  everything                                           7.7 k
 nginx-filesystem                    noarch                 1:1.16.1-2.oe1                  everything                                           8.8 k
 nginx-mod-http-image-filter         x86_64                 1:1.16.1-2.oe1                  everything                                            17 k
 nginx-mod-http-perl                 x86_64                 1:1.16.1-2.oe1                  everything                                            26 k
 nginx-mod-http-xslt-filter          x86_64                 1:1.16.1-2.oe1                  everything                                            16 k
 nginx-mod-mail                      x86_64                 1:1.16.1-2.oe1                  everything                                            45 k
 nginx-mod-stream                    x86_64                 1:1.16.1-2.oe1                  everything                                            68 k

Transaction Summary
==========================================================================================================================================================
Install  14 Packages

Total download size: 1.6 M
Installed size: 5.3 M
Downloading Packages:
(1/14): libunwind-1.3.1-3.oe1.x86_64.rpm                                                                         249 kB/s |  54 kB     00:00
(2/14): gd-2.2.5-6.oe1.x86_64.rpm                                                                                417 kB/s | 142 kB     00:00
(3/14): gperftools-libs-2.7-7.oe1.x86_64.rpm                                                                     745 kB/s | 267 kB     00:00
(4/14): libwebp-1.0.0-5.oe1.x86_64.rpm                                                                           1.3 MB/s | 246 kB     00:00
(5/14): mailcap-2.1.48-6.oe1.noarch.rpm                                                                          570 kB/s |  31 kB     00:00
(6/14): nginx-all-modules-1.16.1-2.oe1.noarch.rpm                                                                143 kB/s | 7.7 kB     00:00
(7/14): nginx-filesystem-1.16.1-2.oe1.noarch.rpm                                                                 163 kB/s | 8.8 kB     00:00
```

**Figure 3-7** Installing Nginx (apt)



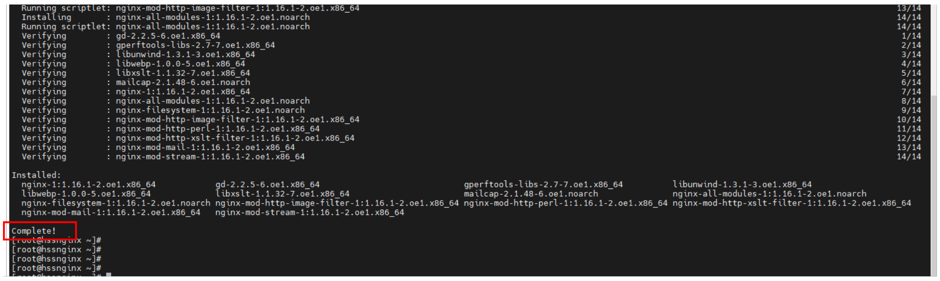
```
Reading package lists...
Building dependency tree...
Reading state information...
The following packages were automatically installed and are no longer required:
  eatmydata libeatmydata1 libflashrom1 libftdi1-2 python-babel-localedata
  python3-babel python3-certifi python3-jinja2 python3-json-pointer
  python3-jsonpatch python3-jsonschema python3-markupsafe python3-pyrsistent
  python3-requests python3-tz python3-urllib3
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  nginx
0 upgraded, 1 newly installed, 0 to remove and 195 not upgraded.
Need to get 3,872 B of archives.
After this operation, 50.2 kB of additional disk space will be used.
Get:1 http://repo.huaweicloud.com/ubuntu jammy-updates/main amd64 nginx amd64 1.18.0-6ubuntu14.4 [3,872 B]
Fetched 3,872 B in 0s (134 kB/s)
```

2. Check whether the Nginx installation is successful.

   – For OSs that support RPM installation, such as EulerOS, CentOS, and Red Hat,

     the installation is automatically performed. If **Complete!** shown in **Nginx installed successfully (rpm)** is displayed, the installation is successful.

     **Figure 3-8** Nginx installed successfully (rpm)

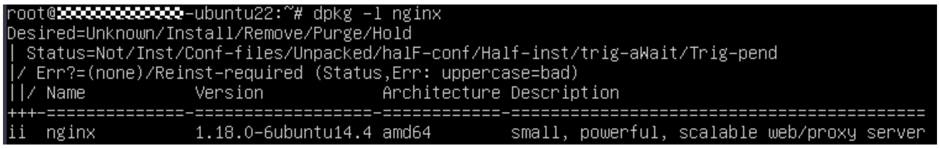
     

```
  Running scriptlet: nginx-mod-http-image-filter-1:1.16.1-2.oe1.x86_64                                                                                13/14
  Installing       : nginx-all-modules-1:1.16.1-2.oe1.noarch                                                                                          14/14
  Running scriptlet: nginx-all-modules-1:1.16.1-2.oe1.noarch                                                                                          14/14
  Verifying        : gd-2.2.5-6.oe1.x86_64                                                                                                             1/14
  Verifying        : gperftools-libs-2.7-7.oe1.x86_64                                                                                                  2/14
  Verifying        : libunwind-1.3.1-3.oe1.x86_64                                                                                                      3/14
  Verifying        : libwebp-1.0.0-5.oe1.x86_64                                                                                                        4/14
  Verifying        : libxslt-1.1.32-7.oe1.x86_64                                                                                                       5/14
  Verifying        : mailcap-2.1.48-6.oe1.noarch                                                                                                       6/14
  Verifying        : nginx-1:1.16.1-2.oe1.x86_64                                                                                                       7/14
  Verifying        : nginx-all-modules-1:1.16.1-2.oe1.noarch                                                                                           8/14
  Verifying        : nginx-filesystem-1:1.16.1-2.oe1.noarch                                                                                            9/14
  Verifying        : nginx-mod-http-image-filter-1:1.16.1-2.oe1.x86_64                                                                                10/14
  Verifying        : nginx-mod-http-perl-1:1.16.1-2.oe1.x86_64                                                                                        11/14
  Verifying        : nginx-mod-http-xslt-filter-1:1.16.1-2.oe1.x86_64                                                                                 12/14
  Verifying        : nginx-mod-mail-1:1.16.1-2.oe1.x86_64                                                                                             13/14
  Verifying        : nginx-mod-stream-1:1.16.1-2.oe1.x86_64                                                                                           14/14

Installed:
  nginx-1:1.16.1-2.oe1.x86_64              gd-2.2.5-6.oe1.x86_64                              gperftools-libs-2.7-7.oe1.x86_64          libunwind-1.3.1-3.oe1.x86_64
  libwebp-1.0.0-5.oe1.x86_64               libxslt-1.1.32-7.oe1.x86_64                        mailcap-2.1.48-6.oe1.noarch               nginx-all-modules-1:1.16.1-2.oe1.noarch
  nginx-filesystem-1:1.16.1-2.oe1.noarch nginx-mod-http-image-filter-1:1.16.1-2.oe1.x86_64 nginx-mod-http-perl-1:1.16.1-2.oe1.x86_64 nginx-mod-http-xslt-filter-1:1.16.1-2.oe1.x86_64
  nginx-mod-mail-1:1.16.1-2.oe1.x86_64     nginx-mod-stream-1:1.16.1-2.oe1.x86_64

Complete!
[root@hssnginx ~]#
[root@hssnginx ~]#
[root@hssnginx ~]#
[root@hssnginx ~]#
[root@hssnginx ~]#
```

   – For OSs that support DEB installation, such as Ubuntu and Debian.

     Run the **pkg –l nginx** command. If the command output shown in **Nginx installed successfully (deb)** is displayed, the installation is successful.

     **Figure 3-9** Nginx installed successfully (deb)

```
root@[redacted]-ubuntu22:~# dpkg -l nginx
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name          Version            Architecture Description
+++-=============-==================-============-=====================================
ii  nginx         1.18.0-6ubuntu14.4 amd64        small, powerful, scalable web/proxy server
```

**Step 4** Configuring CloudNginx

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

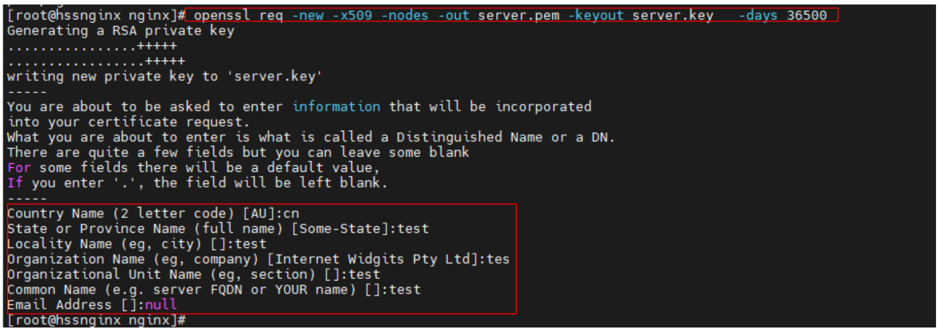
   **cd /etc/nginx/**

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 3-10** Self-signed certificate

```
[root@hssnginx nginx]# openssl req -new -x509 -nodes -out server.pem -keyout server.key   -days 36500
Generating a RSA private key
................+++++
.................+++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:cn
State or Province Name (full name) [Some-State]:test
Locality Name (eg, city) []:test
Organization Name (eg, company) [Internet Widgits Pty Ltd]:tes
Organizational Unit Name (eg, section) []:test
Common Name (e.g. server FQDN or YOUR name) []:test
Email Address []:null
[root@hssnginx nginx]#
```

   NOTE

   The value of **Country Name** can contain only two characters.

3. Run the following command to modify **nginx.conf**:

   a. Run the following command to modify **nginx.conf**:

      **rm -f nginx.conf**

      **vi nginx.conf**

   b. Press **i** to enter the editing mode and copy the following content to the **nginx.conf** file:

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile            on;
    tcp_nopush          on;
    tcp_nodelay         on;
    keepalive_timeout   65;
    types_hash_max_size 2048;

    include             /etc/nginx/mime.types;
    default_type        application/octet-stream;

    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # for more information.
    include /etc/nginx/conf.d/*.conf;

    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;

        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 {
        }
    }
}
```

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

   **:wq!**

d. Run the following command to automatically replace the IP address in the **nginx.conf** file:

   **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**

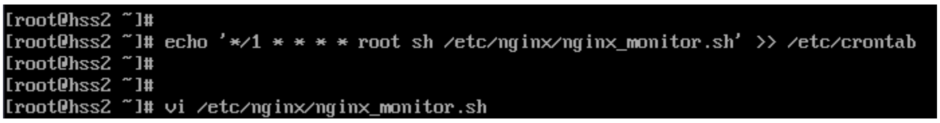
4. Perform the following operations to create the Nginx monitoring script: After the creation is complete, the Nginx running status is checked every minute.

   a. Perform the following commands to create the Nginx monitoring script:

      **echo '*/1 * * * * root sh /etc/nginx/nginx_monitor.sh' >> /etc/crontab**

      **vi /etc/nginx/nginx_monitor.sh**

**Figure 3-11** Creating an Nginx monitoring script

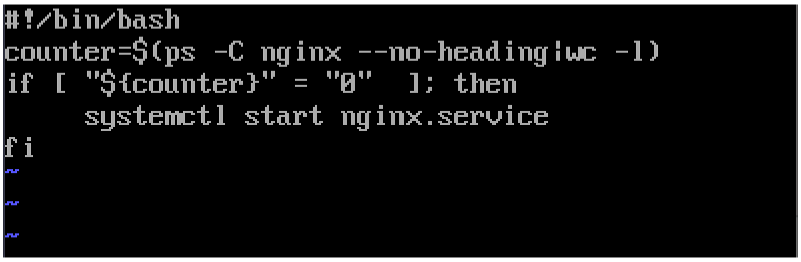


```
[root@hss2 ~]#
[root@hss2 ~]# echo '*/1 * * * * root sh /etc/nginx/nginx_monitor.sh' >> /etc/crontab
[root@hss2 ~]#
[root@hss2 ~]#
[root@hss2 ~]# vi /etc/nginx/nginx_monitor.sh
```

b. Copy the following content to **nginx_monitor.sh**:

```
#!/bin/bash
counter=$(ps -C nginx --no-heading|wc -l)
if [ "${counter}" = "0"  ]; then
    systemctl start nginx.service
fi
```

**Figure 3-12** Configuring **nginx_monitor.sh**



```
#!/bin/bash
counter=$(ps -C nginx --no-heading|wc -l)
if [ "${counter}" = "0"  ]; then
        systemctl start nginx.service
fi
~
~
~
```

c. Enter **ECS**, run the following command, and press **Enter** to exit.

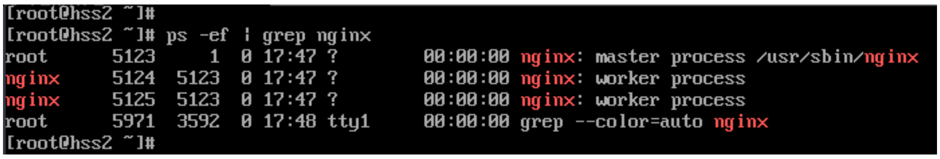
**:wq!**

5. Wait 1 minute and run the following command to check whether the Nginx process has been started successfully:

   **ps -ef | grep nginx**

   If the command output shown in **Nginx process started successfully** is displayed, the Nginx process is started. Perform the **Creating an Agent Installation Package or Installation Commands Using a Proxy Server**.

**Figure 3-13** Nginx process started successfully



```
[root@hss2 ~]#
[root@hss2 ~]# ps -ef | grep nginx
root      5123     1  0 17:47 ?        00:00:00 nginx: master process /usr/sbin/nginx
nginx     5124  5123  0 17:47 ?        00:00:00 nginx: worker process
nginx     5125  5123  0 17:47 ?        00:00:00 nginx: worker process
root      5971  3592  0 17:48 tty1     00:00:00 grep --color=auto nginx
[root@hss2 ~]#
```

**----End**

## 3.4.5 Creating an Agent Installation Package or Installation Commands Using a Proxy Server

Generate the agent installation command for Linux servers and the agent package for Windows servers using a proxy server.

### Creating an Agent Installation Commands Using a Proxy Server (Linux)

**Step 1** Log in to the proxy server.

**Step 2** Run the following command to access the **/tmp** directory:

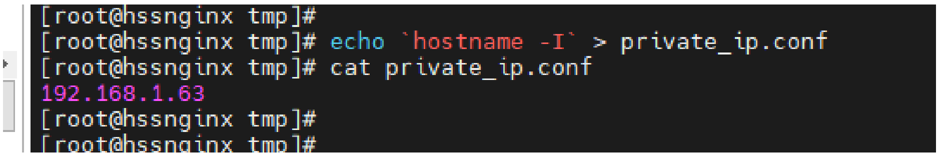
**cd /tmp**

**Step 3** 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 3-14** Viewing IP addresses



```
[root@hssnginx tmp]#
[root@hssnginx tmp]# echo `hostname -I` > private_ip.conf
[root@hssnginx tmp]# cat private_ip.conf
192.168.1.63
[root@hssnginx tmp]#
[root@hssnginx tmp]#
```

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

**Step 4** After confirming that the IP address is available, perform the following operations in sequence to generate the installation command:

1. Run the following commands in sequence to generate the installation commands:
   - 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**

2. Run the following command to replace the available IP address:

   The command needs to be run without modification.

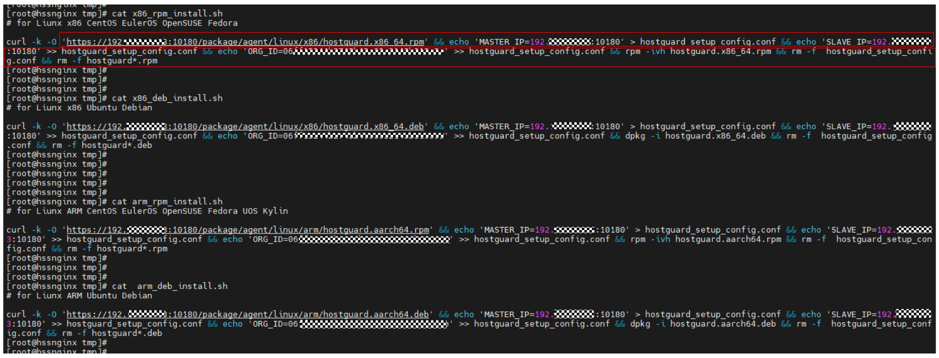
   **sed -i "s#private_ip#`cat private_ip.conf`#g" *install.sh && sed -i "s#project_id#`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2`#g" *install.sh**

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 5** View the generated installation command, which will be used to install agents on the third-party Linux servers.

**Figure 3-15** Linux installation commands



```
[root@hssnginx tmp]#
[root@hssnginx tmp]# cat x86_rpm_install.sh
# for Liunx x86 CentOS EulerOS OpenSUSE Fedora

curl -k -O 'https://192.[redacted]:10180/package/agent/linux/x86/hostguard.x86_64.rpm' && echo 'MASTER_IP=192.[redacted]:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.[redacted]
:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06[redacted]' >> hostguard_setup_config.conf && rpm -ivh hostguard.x86_64.rpm && rm -f  hostguard_setup_confi
g.conf && rm -f hostguard*.rpm
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# cat x86_deb_install.sh
# for Liunx x86 Ubuntu Debian

curl -k -O 'https://192.[redacted]:10180/package/agent/linux/x86/hostguard.x86_64.deb' && echo 'MASTER_IP=192.[redacted]:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.[redacted]
:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06[redacted]' >> hostguard_setup_config.conf && dpkg -i hostguard.x86_64.deb && rm -f  hostguard_setup_config
.conf && rm -f hostguard*.deb
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# cat arm_rpm_install.sh
# for Liunx ARM CentOS EulerOS OpenSUSE Fedora UOS Kylin

curl -k -O 'https://192.[redacted]:10180/package/agent/linux/arm/hostguard.aarch64.rpm' && echo 'MASTER_IP=192.[redacted]:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.[redacted]
3:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06[redacted]' >> hostguard_setup_config.conf && rpm -ivh hostguard.aarch64.rpm && rm -f  hostguard_setup_con
fig.conf && rm -f hostguard*.rpm
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# cat  arm_deb_install.sh
# for Liunx ARM Ubuntu Debian

curl -k -O 'https://192.[redacted]:10180/package/agent/linux/arm/hostguard.aarch64.deb' && echo 'MASTER_IP=192.[redacted]:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.[redacted]
3:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06[redacted]' >> hostguard_setup_config.conf && dpkg -i hostguard.aarch64.deb && rm -f  hostguard_setup_conf
ig.conf && rm -f hostguard*.deb
[root@hssnginx tmp]#
[root@hssnginx tmp]#
```

**----End**

## Creating an Agent Installation Package Using a Proxy Server (Windows)

**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**

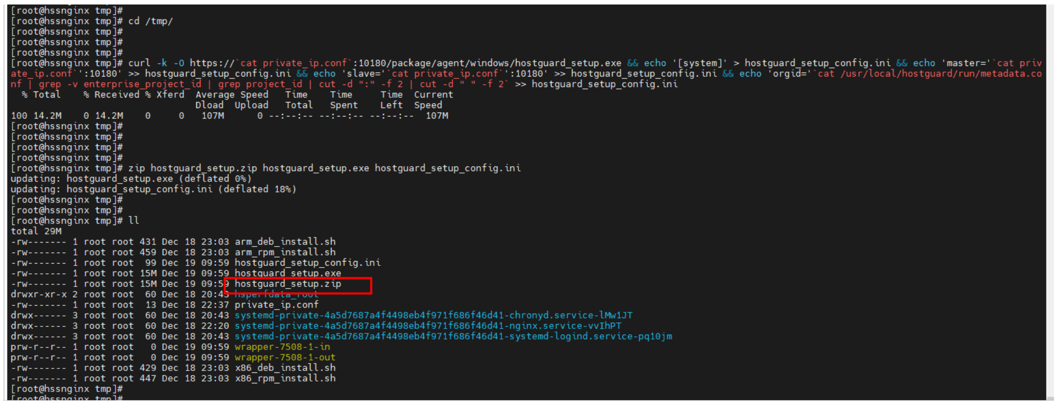
NOTE

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 third-party Windows servers.

**Figure 3-16** Windows installation package



```
[root@hssnginx tmp]#
[root@hssnginx tmp]# cd /tmp/
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# curl -k -O https://`cat private_ip.conf`:10180/package/agent/windows/hostguard_setup.exe && echo '[system]' > hostguard_setup_config.ini && echo 'master='`cat priv
ate_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.co
nf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2` >> hostguard_setup_config.ini
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 14.2M    0 14.2M    0     0   107M      0 --:--:-- --:--:-- --:--:--  107M
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# zip hostguard_setup.zip hostguard_setup.exe hostguard_setup_config.ini
updating: hostguard_setup.exe (deflated 0%)
updating: hostguard_setup_config.ini (deflated 18%)
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# ll
total 29M
-rw------- 1 root root 431 Dec 18 23:03 arm_deb_install.sh
-rw------- 1 root root 459 Dec 18 23:03 arm_rpm_install.sh
-rw------- 1 root root  99 Dec 19 09:59 hostguard_setup_config.ini
-rw------- 1 root root 15M Dec 19 09:59 hostguard_setup.exe
-rw------- 1 root root 15M Dec 19 09:59 hostguard_setup.zip
drwxr-xr-x 2 root root  60 Dec 18 20:43 hsperfdata_root
-rw------- 1 root root  13 Dec 18 22:37 private_ip.conf
drwx------ 3 root root  60 Dec 18 20:43 systemd-private-4a5d7687a4f4498eb4f971f686f46d41-chronyd.service-lMw1JT
drwx------ 3 root root  60 Dec 18 22:20 systemd-private-4a5d7687a4f4498eb4f971f686f46d41-nginx.service-vvIhPT
drwx------ 3 root root  60 Dec 18 20:43 systemd-private-4a5d7687a4f4498eb4f971f686f46d41-systemd-logind.service-pq10jm
prw-r--r-- 1 root root   0 Dec 19 09:59 wrapper-7508-1-in
prw-r--r-- 1 root root   0 Dec 19 09:59 wrapper-7508-1-out
-rw------- 1 root root 429 Dec 18 23:03 x86_deb_install.sh
-rw------- 1 root root 447 Dec 18 23:03 x86_rpm_install.sh
[root@hssnginx tmp]#
[root@hssnginx tmp]#
```

**----End**

# 3.4.6 Installing an Agent for a Third-Party Server

Install agents on third-party servers and manage the servers in HSS in a unified manner.

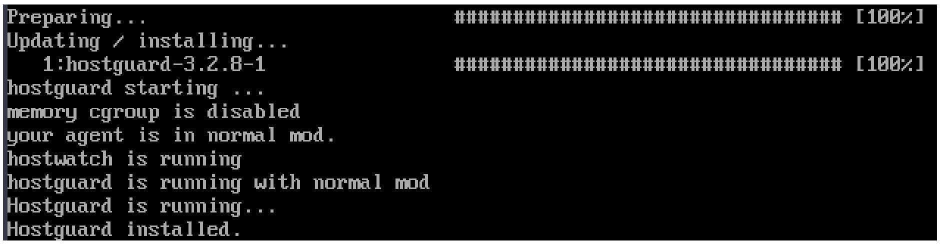
## Installing the Agent for a Third-Party Linux Server

**Step 1** Copy the Linux installation commands in **Creating an Agent Installation Commands Using a Proxy Server (Linux)**.

**Step 2** Log in to the target third-party Linux server as user **root**, paste and run the Linux installation command.

If the command output shown in **Installing an agent** is displayed, the agent has been installed.

**Figure 3-17** 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** Wait for about 10 minutes. In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The ECS page is displayed.

**Step 4** If the target server is displayed in the server list, the connection is successful.

**----End**

## Installing the Agent for a Third-Party Windows Server

**Step 1** Copy the Windows installation package created in section **Creating an Agent Installation Package Using a Proxy Server (Windows)** to the local PC.

**Step 2** Upload the installation package to the target third-party Windows server where the agent is to be installed.

**Step 3** Log in to the third-party server using the Administrator account.

**Step 4** Decompress the installation package, double-click **hostguard_setup.exe**, and install the agent according to the installation wizard.

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.

**Step 5** After the installation is complete, if the **HostGuard.exe** and **HostWatch.exe** processes are displayed in the Windows Task Manager, the agent is successfully installed.

**Step 6** Wait for about 10 minutes. In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The ECS page is displayed.

**Step 7** If the target server is displayed in the server list, the connection is successful.

**----End**

# 4 Connecting Third-Party Servers to HSS Through Direct Connect and VPC Endpoint

## 4.1 Overview

### Scenario

With the development of hybrid clouds, there is also a growing need for companies to perform unified security management of on- and off-cloud or hybrid clouds. HSS supports the access and management of third-party cloud servers and on-premises IDCs. Users are allowed to use the same security policies on different clouds, preventing the risks caused by inconsistent security policies.

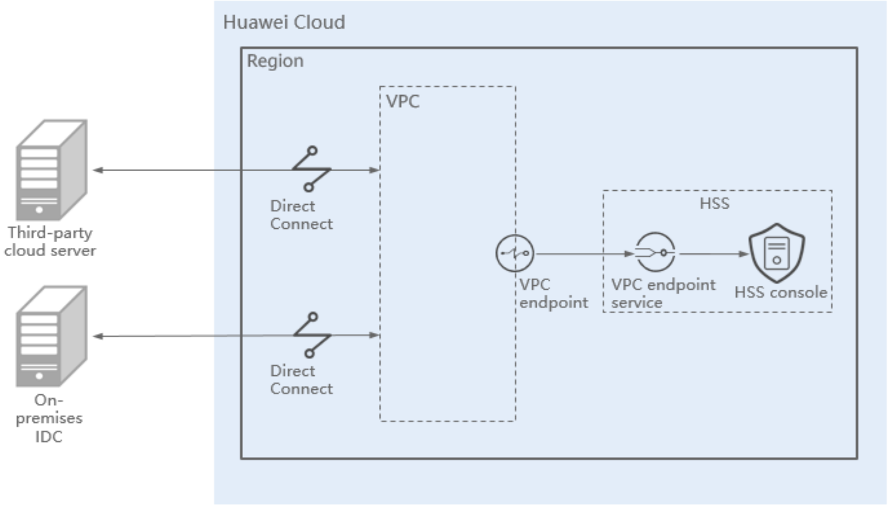
If your server cannot access the Internet, you can refer to this solution to connect your server to HSS through **Direct Connect and VPC Endpoint** for protection management. If your server can access the Internet, connect the server to HSS by referring to **Installing the Agent for a Third-Party Server**.

### Architecture

Third-party servers communicate with VPCs on the cloud through Direct Connect, and then connect to HSS through VPC endpoint, as shown in **Connecting a third-party server to HSS through Direct Connect and VPC endpoint**.

- **Direct Connect** establishes a dedicated network connection that features high speed, low latency, stability, and security between your on-premises data center and Huawei Cloud VPC. Direct Connect allows you to maximize legacy IT facilities and leverage cloud services to build a flexible, scalable hybrid cloud compute environment.
- **VPC Endpoint** enables you to access Huawei Cloud services or your own private services securely. It provides flexible networking without having to use EIPs.

**Figure 4-1** Connecting third-party servers to HSS through Direct Connect and VPC endpoint



## Advantages

Compared with the **Third-Party Servers Accessing HSS Through a Direct Connect and Proxy Servers** solution, this solution does not require creating a proxy server or configuring Nginx, simplifying operations and reducing costs.

## Limitations and Constraints

Currently, only **CN East 2** and **Southwest-Guiyang 1** are supported. Third-party servers can access HSS through Direct Connect and VPC endpoint.

# 4.2 Resources and Costs

The following table lists resources in this example.

**Table 4-1** Description

| Resource | Description | Quantity | Cost |
|---|---|---|---|
| Direct Connect | Direct Connect is used to connect third-party servers and cloud resources. | 2 | For detailed billing modes and billing standards, see **Billing**. |

| Resource | Description | Quantity | Cost |
|---|---|---|---|
| VPC Endpoint (VPCEP) | VPCEP provides channels to connect your VPC to VPC endpoint services so that third-party servers can access HSS through the Huawei Cloud intranet. | 1 | Free |

# 4.3 Process Flow

The process for third-party cloud servers and on-premises IDC to access HSS through Direct Connect and VPC endpoint is as follows:

1. **Creating a Direct Connect**

   If a third-party server cannot access the public network, you need to create a Direct Connect connection to connect to the VPC for network interconnection.

2. **Creating a VPC Endpoint**

   Create a VPC endpoint to enable third-party servers to access HSS through the Huawei Cloud intranet.

3. **Obtaining a Project ID**

   Obtain the ID of the project to which the VPC endpoint belongs, which is used to generate the installation command.

4. **Creating the Agent Installation Package or Installation Command**

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

5. **Installing an Agent for a Third-Party Server**

   Install an agent for the third-party server and connect the server to HSS for unified management.

# 4.4 Process

## 4.4.1 Creating a Direct Connect

Third-party servers and on-premises IDCs can use Direct Connect to access servers in VPCs on the cloud without using the public network.

For details about Direct Connect, see **Direct Connect Introduction**.

### Creating a Direct Connect

For details, see **Using Direct Connect to Connect an On-Premises Data Center to the Cloud**.

**Step 1** Create a connection.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the region and project.
3. Click ☰ in the upper left corner of the page and choose **Networking** > **Direct Connect** to switch to the **Connections** page.
4. Click **Create Connection**.
5. On the **Create Connection** page, enter the equipment room details and select the Direct Connect location and port based on **Table 4-2**.

**Table 4-2** Parameters required for creating a cloud connection

| Parameter | Description |
|---|---|
| Billing Mode | Specifies how you are charged. Currently, only **Yearly/Monthly** is supported. |
| Region | Specifies the region where the connection is deployed. You can change the region in the upper left corner of the console. |
| Connection Name | Specifies the name of your connection. |
| Location | Specifies the location where your leased line can connect to. |
| Carrier | Specifies the carrier that provides the leased line. |
| Port Type | Specifies the type of the port used by the connection. There are four types of ports: 1GE, 10GE, 40GE, and 100GE. |
| Leased Line Bandwidth | Specifies the bandwidth of the leased line in the unit of Mbit/s. This is the bandwidth of the leased line you bought from the carrier. |
| Your Equipment Room Address | Specifies the address of your equipment room. The address must be specific to the floor your equipment room is on, |

| Parameter | Description |
|---|---|
| Tag | Identifies the connection. A tag consists of a key and a value. You can add 10 tags to a connection.<br>**NOTE**<br>If a predefined tag has been created in TMS, you can select the corresponding tag key and value.<br>For details about predefined tags, see **Predefined Tag Overview**. |
| Description | Provides supplementary information about the connection. |
| Contact Person/Phone Number/ Email | Specifies information about the person who is responsible for your connection.<br>If no contact information is provided, we will contact the person in your account information. This will prolong the review period. |
| Required Duration | Specifies how long the connection will be used for. |
| Auto-renewing DBSS | Specifies whether to automatically renew the connection to ensure service continuity.<br>It is recommended that you set the auto-renewal period to be the same as the required duration. If the required duration is three months, the system automatically renews the subscription for every three months. |
| Enterprise Project | Specifies an enterprise project by which cloud resources and members are centrally managed. |

6. Click **Confirm Configuration**.
7. Confirm the configuration and click **Request Connection**.

   Confirm the requirements with the Direct Connect manager.
8. After the system approves the requirement, the user needs to contact the carrier for construction.

   After the construction is complete, locate the connection in the connection list and click **Confirm Cabling** in the **Operation** column.
9. In the displayed dialog box, click **OK**.
10. In the connection list, locate the connection and click **Confirm Configuration** in the **Operation** column.
11. Confirm the configuration and click **Pay Now**.

12. Confirm the order, select a payment method, and click **Confirm**.
13. After the payment is complete, wait for Huawei Cloud to complete the construction.

    Huawei onsite engineers will connect the Direct Connect connection to the Huawei Cloud gateway port based on the customer information within two working days.
14. Verify that the connection is in the **Normal** state, which means that the connection is ready, and the billing starts.

**Step 2** Create a virtual gateway.

1. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**.
2. In the upper right corner of the **Virtual Gateways** page, click **Create Virtual Gateway**.
3. Configure the virtual gateway parameters.

**Table 4-3** Virtual gateway parameters

| Parameter | Description |
|---|---|
| Name | Specifies the virtual gateway name.<br>You can enter 1 to 64 characters. |
| Enterprise Project | Specifies the enterprise project by which virtual gateways are centrally managed. Select an existing enterprise project. |
| VPC | Specifies the VPC to be associated with the virtual gateway. |
| Subnet CIDR Block | Specifies CIDR blocks of the VPC subnets.<br>You can enter one or more CIDR blocks and separate every entry with a comma (,). |
| BGP ASN | Specifies the BGP ASN of the virtual gateway. |
| Tag | Adds tags to help you identify your virtual gateway. You can change them after the virtual gateway is created. |
| Description | Provides supplementary information about the virtual gateway. |

4. Click **OK**.

**Step 3** Create a virtual interface.

1. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.
2. Click **Create Virtual Interface**.
3. Configure the parameters as prompted.

**Table 4-4** Parameters for creating a virtual interface

| Parameter | Description |
|---|---|
| Region | Specifies the region where the connection is deployed. You can change the region in the upper left corner of the console. |
| Name | Specifies the virtual interface name.<br>The name can contain 1 to 64 characters. |
| Virtual Interface Priority | Specifies whether the virtual interface will be used prior to other virtual interfaces. There are two options: **Preferred** and **Standard**.<br>If multiple virtual interfaces are associated with one Direct Connect device, the load is balanced among virtual interfaces with the same priority, while virtual interfaces with different priorities are working in active/ standby pairs. |
| Connection | Specifies the connection you use to connect your data center to the cloud. |
| Gateway | Specifies the gateway that the virtual interface connects to.<br>You can select a virtual gateway or global DC gateway. |
| Virtual Gateway | This parameter is mandatory when **Gateway** is set to **Virtual gateway**.<br>Specifies the virtual gateway that the virtual interface connects to. |
| Global DC Gateway | This parameter is mandatory when **Gateway** is set to **Global DC gateway**.<br>Specifies the global DC gateway that the virtual interface connects to. |
| VLAN | Specifies the ID of the VLAN for the virtual interface.<br>You need to configure the VLAN if you create a standard connection.<br>The VLAN for a hosted connection will be allocated by the carrier or partner. You do not need to configure the VLAN. |
| Bandwidth | Specifies the bandwidth that can be used by the virtual interface in the unit of Mbit/s. The bandwidth cannot exceed that of the connection. |
| Enterprise Project | Specifies the enterprise project by which virtual interfaces are centrally managed. Select an existing enterprise project. |
| Tag | Adds tags to help you identify your virtual interface. You can change them after the virtual interface is created. |

| Parameter | Description |
|---|---|
| Local Gateway | Specifies the IP address used by the cloud to connect to your on-premises network. After you configure **Local Gateway** on the console, the configuration will be automatically delivered to the gateway used by the cloud. |
| Remote Gateway | Specifies the IP address used by the on-premises data center to connect to the cloud. After you configure **Remote Gateway** on the console, you need to configure the IP address on the interface of the on-premises device. |
| Remote Subnet | Specifies the subnets of your on-premises network. Separate every entry with a comma (,). |
| Routing Mode | Specifies the routing mode. Two options are available, **Static** and **BGP**.<br>If there are two or more connections, select BGP routing. |
| BGP ASN | Specifies the ASN of the BGP peer.<br>This parameter is mandatory when you select BGP routing. |
| BGP MD5 Authentication Key | Specifies the password used to authenticate the BGP peer using MD5.<br>This parameter can be set when BGP routing is selected, and the parameter values on both gateways must be the same.<br>The key contains 8 to 255 characters and must contain at least two types of the following characters:<br>– Uppercase letter<br>– Lowercase letter<br>– Digits<br>– Special characters ~!, .:;-_"(){}[]/@#$ %^&*+\\|= |
| Description | Provides supplementary information about the virtual interface. |

4. Click **Create Now**.

   When the status changes to **Normal**, the virtual interface has been created.

**Step 4** Configure local routes on the on-premises data centers.

After your on-premises network is connected to Huawei Cloud, you need to configure routes in your data center.

- For details about how to configure static routes, see **Accessing a VPC Using a Static Routing Connection**.

- For details about how to configure BGP routes, see **Accessing a VPC Using a BGP Routing Connection**.

**----End**

## 4.4.2 Creating a VPC Endpoint

Create a VPC endpoint to enable third-party servers to access HSS through the Huawei Cloud intranet. Create a VPC endpoint will occupy a VPC subnet IP address. Only one VPC endpoint needs to be created for each VPC.

### Creating a VPC Endpoint

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

**Step 2** Click 📍 in the upper left corner and select the region and project.

**Step 3** Click ☰ in the upper left corner of the page and choose **Networking** > **VPC Endpoint** to switch to the **VPC Endpoint** page.

**Step 4** In the upper right corner of the page, click **Buy VPC Endpoint**.

**Step 5** Set the parameters.

1. **Region**: Select **CN East2** or **CN Southwest-Guiyang1**. Set the parameter based on the region to which the server is connected.
2. **Service Category**: Select **Cloud service**.
3. Selecting a service
   - Select **com.myhuaweicloud.xxx.hss-agent**. **xxx** indicates the region ID. For example, the region ID of CN East 2 is **cn-east-4**.
   - Select **Create a Private Domain Name**.
4. **VPC**: Select a VPC that communicates with your server.
5. **Subnet**: Select or create a subnet.
6. **IPv4 Address**: Select **Automatically assign IP address**.
7. Other parameters: Set parameters as prompted.

**Step 6** Click **Next** to submit the order.

**Step 7** Return to the **VPC Endpoints** page, confirm that the VPC endpoint is created, and obtain and record the service address (IP address).

The service address is required when you create an installation package or generate an installation command.

**----End**

## 4.4.3 Obtaining a Project ID

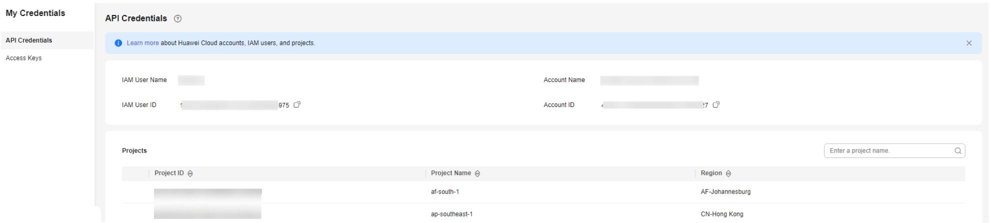
**Step 1** Log in to the management console.

**Step 2** Hover the pointer over the username in the upper right corner and choose **My Credentials** from the drop-down list.

**Step 3** On the **API Credentials** page, obtain the project ID in the project list.

Obtain the project ID of the region to which the created VPC endpoint belongs.

**Figure 4-2** Obtaining a project ID



My Credentials

API Credentials

Access Keys

API Credentials

Learn more about Huawei Cloud accounts, IAM users, and projects.

IAM User Name [redacted]

Account Name [redacted]

IAM User ID 1[redacted]975

Account ID 4[redacted]27

Projects

Enter a project name.

| Project ID | Project Name | Region |
|---|---|---|
| [redacted] | af-south-1 | AF-Johannesburg |
| [redacted] | ap-southeast-1 | CN-Hong Kong |

**----End**

# 4.4.4 Generating the Agent Installation Package or Installation Command

Use a Linux server to generate the agent installation command (Linux) or agent installation package (Windows).

## Generating the Agent Installation Command (Linux)

**Step 1** Log in to any Linux server.

**Step 2** Run the following command to access the **/tmp** directory:

**cd /tmp**

**Step 3** Run the following commands in sequence to write the VPC endpoint IP address to the **private_ip.conf** file and the project ID to the **project_id.conf** file:

**echo "{VPC endpoint ip}" > private_ip.conf**

**cat private_ip.conf**

**echo "{project ID}" > project_id.conf**

**cat project_id.conf**

NOTICE

Set the **IP address** and **Project ID** in the preceding command as required.

- The VPC endpoint IP address is the service address obtained when the **Creating a VPC Endpoint** operation is performed.
- The project ID is the one you obtained when performing the **Obtaining a Project ID** operation.

**Step 4** Perform the following operations in sequence to generate installation commands:

1. Run the following commands in sequence to generate the installation commands:
   - 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
  ```

2. Run the following command to replace the VPC endpoint IP address and project ID:

   The command needs to be run without modification.

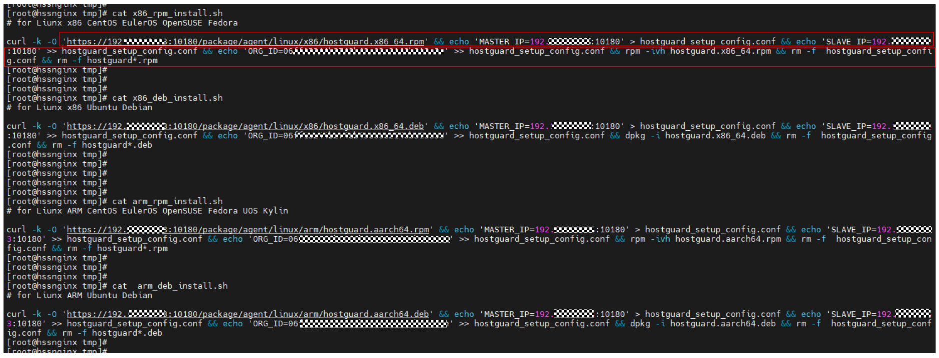
   ```
   sed -i "s#private_ip#`cat private_ip.conf`#g" *install.sh && sed -i "s#project_id#`cat project_id.conf`#g" *install.sh
   ```

NOTE

- All the preceding five commands must be executed. The last command for replacing the VPC endpoint IP address and project 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 5** View the generated installation command, which will be used to install agents on the third-party Linux servers.

**Figure 4-3** Linux installation commands



```
[root@hssnginx tmp]#
[root@hssnginx tmp]# cat x86_rpm_install.sh
# for Liunx x86 CentOS EulerOS OpenSUSE Fedora

curl -k -O 'https://192[redacted]:10180/package/agent/linux/x86/hostguard.x86_64.rpm' && echo 'MASTER_IP=192.[redacted]:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.[redacted]
:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06[redacted]' >> hostguard_setup_config.conf && rpm -ivh hostguard.x86_64.rpm && rm -f  hostguard_setup_confi
g.conf && rm -f hostguard*.rpm
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# cat x86_deb_install.sh
# for Liunx x86 Ubuntu Debian

curl -k -O 'https://192.[redacted]:10180/package/agent/linux/x86/hostguard.x86_64.deb' && echo 'MASTER_IP=192.[redacted]:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.[redacted]
:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06[redacted]' >> hostguard_setup_config.conf && dpkg -i hostguard.x86_64.deb && rm -f  hostguard_setup_config
.conf && rm -f hostguard*.deb
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# cat arm_rpm_install.sh
# for Liunx ARM CentOS EulerOS OpenSUSE Fedora UOS Kylin

curl -k -O 'https://192.[redacted]:10180/package/agent/linux/arm/hostguard.aarch64.rpm' && echo 'MASTER_IP=192.[redacted]:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.[redacted]
:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06[redacted]' >> hostguard_setup_config.conf && rpm -ivh hostguard.aarch64.rpm && rm -f  hostguard_setup_con
fig.conf && rm -f hostguard*.rpm
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# cat  arm_deb_install.sh
# for Liunx ARM Ubuntu Debian

curl -k -O 'https://192.[redacted]:10180/package/agent/linux/arm/hostguard.aarch64.deb' && echo 'MASTER_IP=192.[redacted]:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.[redacted]
:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06[redacted]' >> hostguard_setup_config.conf && dpkg -i hostguard.aarch64.deb && rm -f  hostguard_setup_conf
ig.conf && rm -f hostguard*.deb
[root@hssnginx tmp]#
[root@hssnginx tmp]#
```

**----End**

## Generating an Agent Installation Package (Windows)

**Step 1** Log in to any Linux server.

**Step 2** Run the following command to access the **/tmp** directory:

**cd /tmp**

**Step 3** 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
```

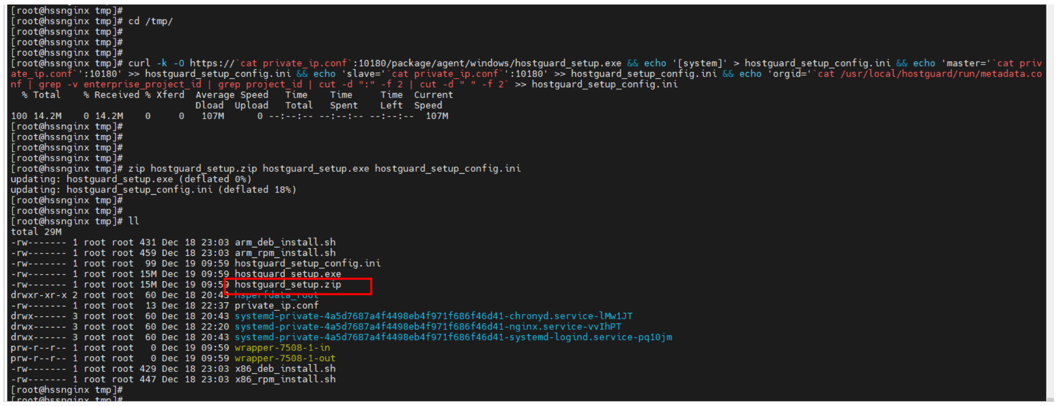
NOTE

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

**yum install -y zip**

**Step 4** View the generated installation package, which will be used to install agents on the third-party Windows servers.

**Figure 4-4** Windows installation package



```
[root@hssnginx tmp]#
[root@hssnginx tmp]# cd /tmp/
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# curl -k -O https://`cat private_ip.conf`:10180/package/agent/windows/hostguard_setup.exe && echo '[system]' > hostguard_setup_config.ini && echo 'master='`cat priv
ate_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.co
nf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2` >> hostguard_setup_config.ini
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 14.2M    0 14.2M    0     0   107M      0 --:--:-- --:--:-- --:--:--  107M
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# zip hostguard_setup.zip hostguard_setup.exe hostguard_setup_config.ini
updating: hostguard_setup.exe (deflated 0%)
updating: hostguard_setup_config.ini (deflated 18%)
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# ll
total 29M
-rw------- 1 root root 431 Dec 18 23:03 arm_deb_install.sh
-rw------- 1 root root 459 Dec 18 23:03 arm_rpm_install.sh
-rw------- 1 root root  99 Dec 19 09:59 hostguard_setup_config.ini
-rw------- 1 root root 15M Dec 19 09:59 hostguard_setup.exe
-rw------- 1 root root 15M Dec 19 09:59 hostguard_setup.zip
drwxr-xr-x 2 root root  60 Dec 18 20:43 hsperfdata_root
-rw------- 1 root root  13 Dec 18 22:37 private_ip.conf
drwx------ 3 root root  60 Dec 18 20:43 systemd-private-4a5d7687a4f4498eb4f971f686f46d41-chronyd.service-lMw1JT
drwx------ 3 root root  60 Dec 18 22:20 systemd-private-4a5d7687a4f4498eb4f971f686f46d41-nginx.service-vvIhPT
drwx------ 3 root root  60 Dec 18 20:43 systemd-private-4a5d7687a4f4498eb4f971f686f46d41-systemd-logind.service-pq10jm
prw-r--r-- 1 root root   0 Dec 19 09:59 wrapper-7508-1-in
prw-r--r-- 1 root root   0 Dec 19 09:59 wrapper-7508-1-out
-rw------- 1 root root 429 Dec 18 23:03 x86_deb_install.sh
-rw------- 1 root root 447 Dec 18 23:03 x86_rpm_install.sh
[root@hssnginx tmp]#
[root@hssnginx tmp]#
```

**----End**

# 4.4.5 Installing an Agent for a Third-Party Server

Install agents on third-party servers and manage the servers in HSS in a unified manner.

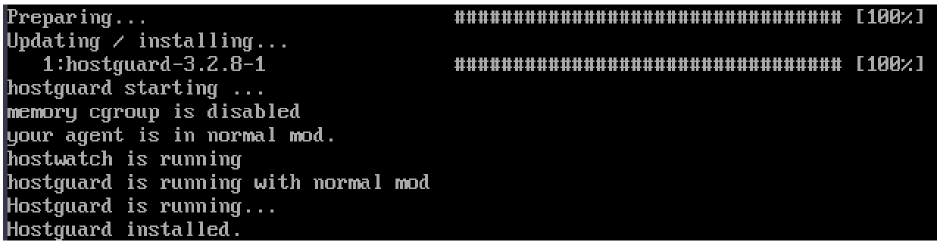
## Installing the Agent for a Third-Party Linux Server

**Step 1** Copy the Linux installation commands in **Generating the Agent Installation Command (Linux)**.

**Step 2** Log in to the target third-party Linux server as user **root**, paste and run the Linux installation command.

If the command output shown in **Installing an agent** is displayed, the agent has been installed.

**Figure 4-5** 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** Wait for about 10 minutes. In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The ECS page is displayed.

**Step 4** If the target server is displayed in the server list, the connection is successful.

**----End**

## Installing the Agent for a Third-Party Windows Server

**Step 1** Copy the Windows installation package created in section **Generating an Agent Installation Package (Windows)** to the local PC.

**Step 2** Upload the installation package to the target third-party Windows server where the agent is to be installed.

**Step 3** Log in to the third-party server using the Administrator account.

**Step 4** Decompress the installation package, double-click **hostguard_setup.exe**, and install the agent according to the installation wizard.

> **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.

**Step 5** After the installation is complete, if the **HostGuard.exe** and **HostWatch.exe** processes are displayed in the Windows Task Manager, the agent is successfully installed.

**Step 6** Wait for about 10 minutes. In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The ECS page is displayed.

**Step 7** If the target server is displayed in the server list, the connection is successful.

**----End**

# 5 Installing the HSS Agent Using CBH

## Scenario

If you have purchased the Huawei Cloud Cloud Bastion Host (CBH) professional edition, you can use CBH to install the HSS 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.

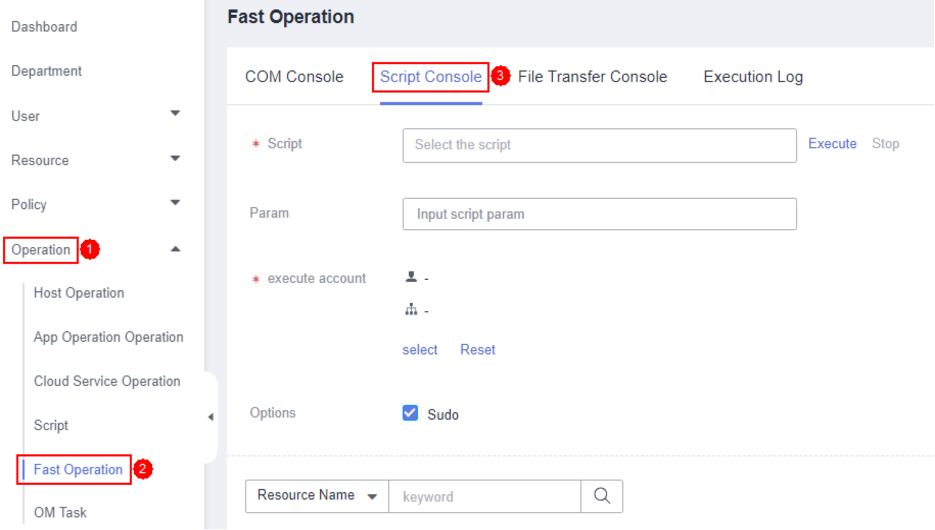
## Procedure

**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

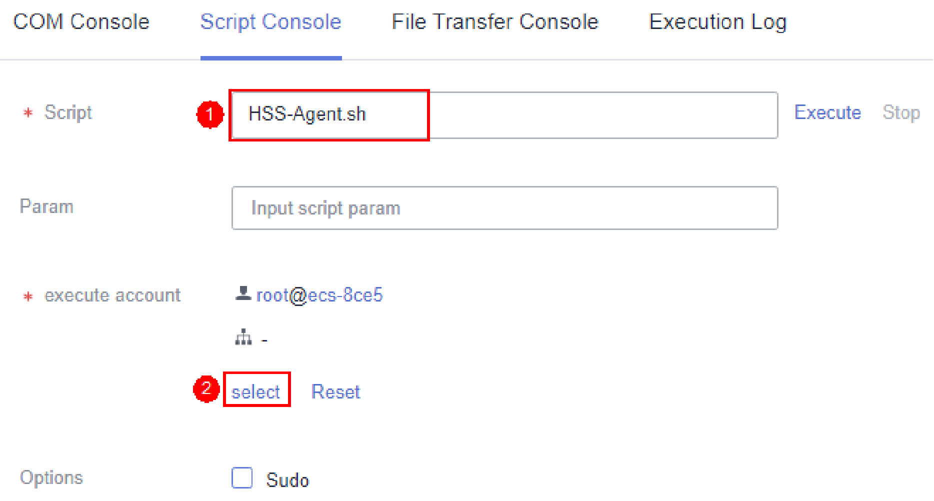
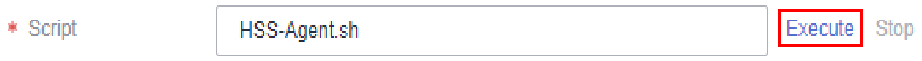


**Table 5-1** Script O&M parameters

| Parameter | Description |
|---|---|
| Script | Select the **HSS-Agent.sh** script. |
| Param | Leave this parameter blank. |
| Execution 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**.

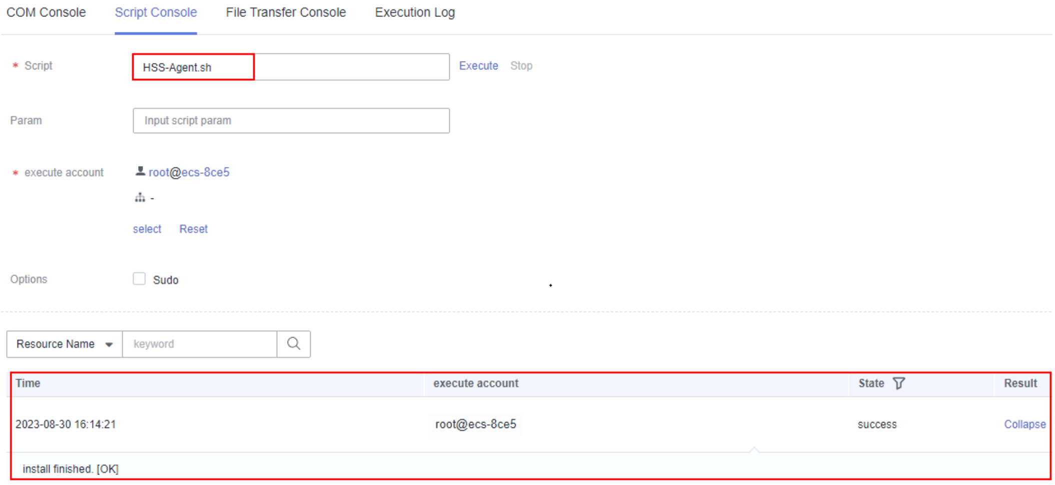
**Figure 5-3** Executing a script task



**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



| Time | execute account | State | Result |
|---|---|---|---|
| 2023-08-30 16:14:21 | root@ecs-8ce5 | success | Collapse |

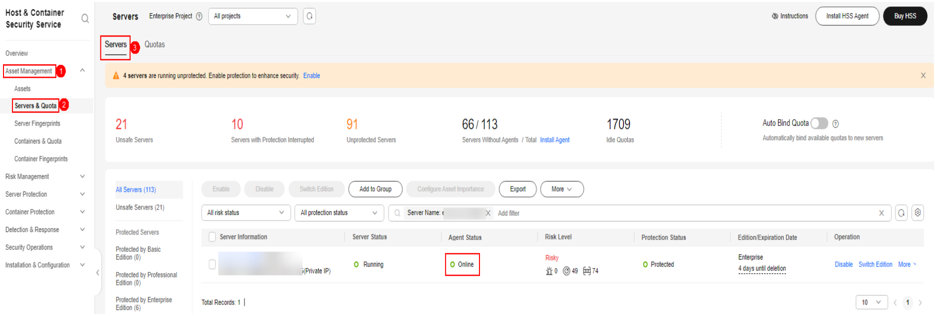
```
install finished. [OK]
```

**Step 7** On the HSS console, confirm the agent installation result.

1. Log in to the HSS 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



| Server Information | Server Status | Agent Status | Risk Level | Protection Status | Edition/Expiration Date | Operation |
|---|---|---|---|---|---|---|
| [redacted] (Private IP) | Running | Online | Risky<br>0 49 74 | Protected | Enterprise<br>4 days until deletion | Disable Switch Edition More |

**----End**

# 6 Using HSS to Improve Server Login Security

## Scenario

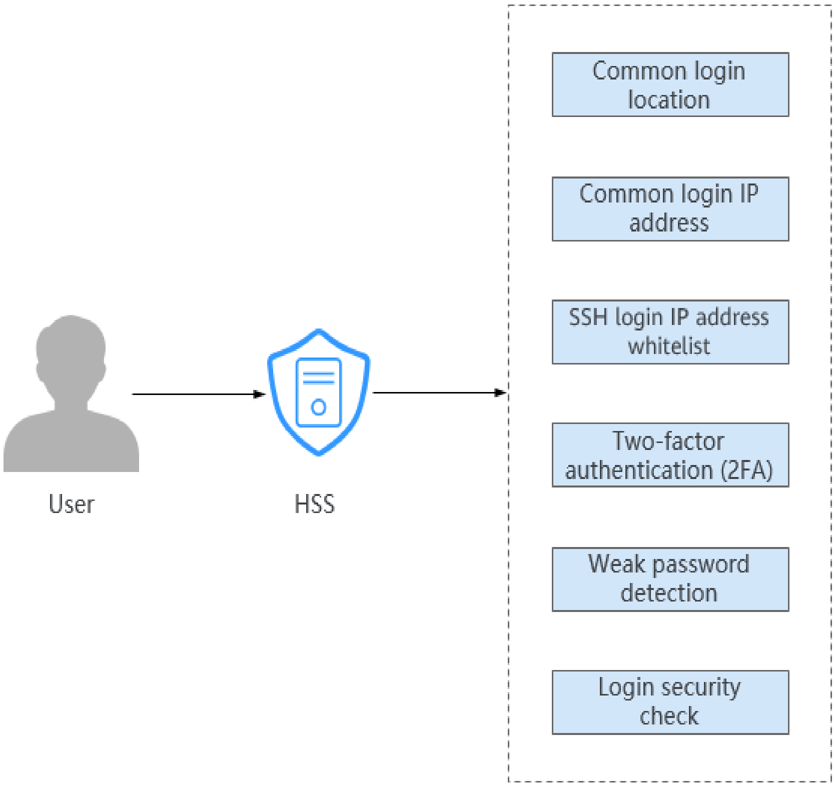
Account and password cracking are the most commonly used ways for attackers to intrude or attack servers. Enhancing login security is the first step to protect server security and ensure that services can run properly.

This section describes how to use HSS to improve server login security.

## Solution Architecture and Advantages

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.

**Figure 6-1** Security hardening for server logins



- Common login location

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

- Common login IP address

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

- SSH login IP address whitelist

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

- Two-factor authentication (2FA)

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

- 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.

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

- Login security check

  After login security detection policy 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.

## Prerequisites

HSS Professional, Enterprise, Premium, Web Tamper Protection, or Container Edition has been enabled for the server. For details, see **HSS Access Overview**.

## Limitations and Constraints

- If 2FA is enabled, it can be used only in following scenarios:
  - Linux: The SSH password is used to log in to an ECS, and the OpenSSH version is earlier than 8.
  - Windows: The RDP file is used to log in to a Windows ECS.
- When two-factor authentication is enabled for Windows servers, the **User must change password at next logon** function is not allowed. To use this function, disable two-factor authentication.
- On a Windows server, 2FA may conflict with G01 and 360 Guard (server edition). You are advised to stop them.

## Process

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

**Step 2** Click in the upper left corner and select the region and project.

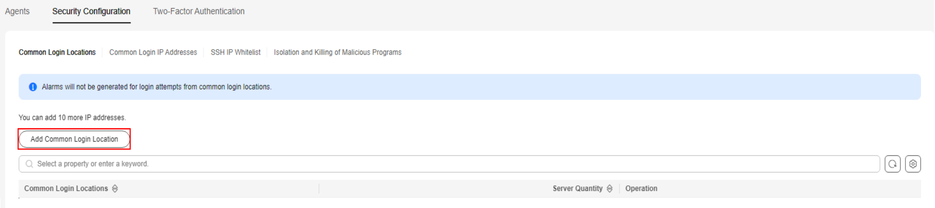
**Step 3** Click ☰ in the upper left corner of the page and choose **Security & Compliance** > HSS.

**Step 4** **Configuring common login locations**

An account can add up to 10 common login locations.

1. In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.
2. Choose **Security Configuration** > **Common Login Location** tab. The **Common Login Location** page is displayed.
3. Choose **Add Common Login Location**.

**Figure 6-2** Adding a common login location


Agents
Security Configuration
Two-Factor Authentication
Common Login Locations
Common Login IP Addresses
SSH IP Whitelist
Isolation and Killing of Malicious Programs
Add Common Login Location
Select a property or enter a keyword.
Common Login Locations
Server Quantity
Operation

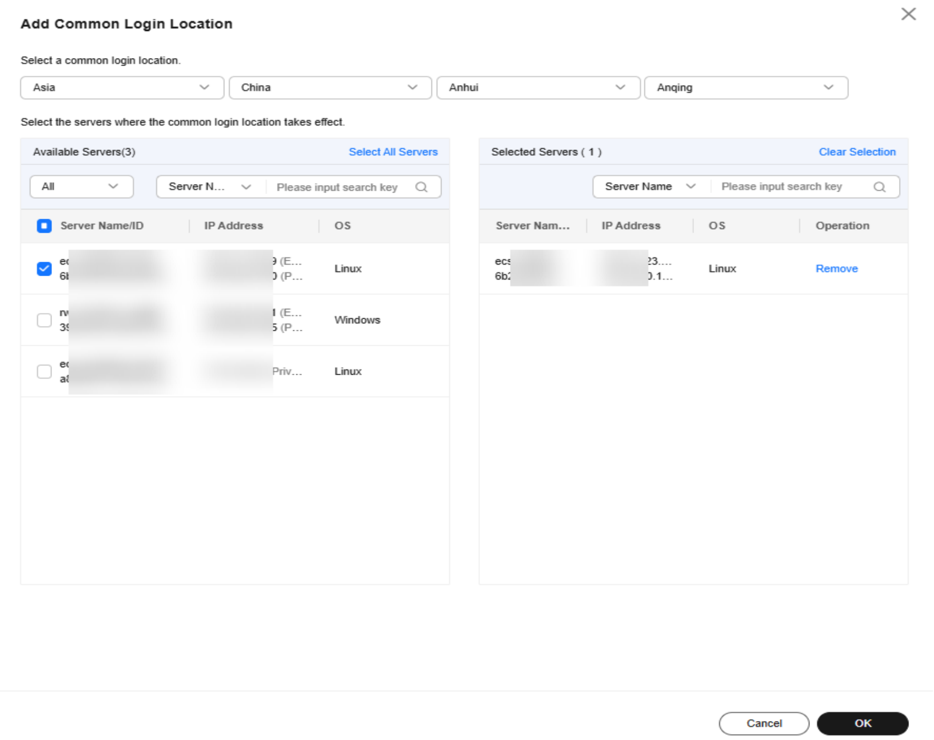
Alarms will not be generated for login attempts from common login locations.

You can add 10 more IP addresses.

4. In the dialog box, select the common login location to be added and the server where the common login location takes effect. After confirming that the information is correct, click **OK**.

   You can select multiple servers where the common login location takes effect.

**Figure 6-3** Configuring common login locations



Add Common Login Location

Select a common login location.

Asia | China | Anhui | Anqing

Select the servers where the common login location takes effect.

Available Servers(3) — Select All Servers

All | Server N... | Please input search key

| ☑ Server Name/ID | IP Address | OS |
|---|---|---|
| ☑ ec 6l [redacted] | [redacted] 9 (E... 0 (P... | Linux |
| □ rv 39 [redacted] | [redacted] 1 (E... 5 (P... | Windows |
| □ ec a8 [redacted] | [redacted] Priv... | Linux |

Selected Servers ( 1 ) — Clear Selection

Server Name | Please input search key

| Server Nam... | IP Address | OS | Operation |
|---|---|---|---|
| ecs 6b [redacted] | [redacted] 23.... 0.1... | Linux | Remove |

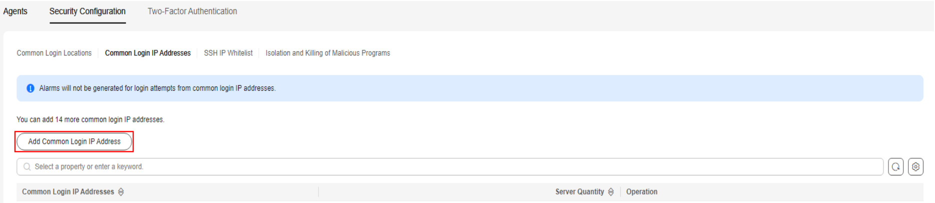
5. Return to the Common Login Locations sub-tab and check the added common login locations.

**Step 5 Configuring common login IP addresses**

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

1. Choose **Security Configuration** > **Common Login IP Addresses** tab. The **Common Login IP Addresses** page is displayed.
2. Choose **Add Common Login IP Addresses**.

**Figure 6-4** Adding a common login IP address



Agents
Security Configuration
Two-Factor Authentication
Common Login Locations
Common Login IP Addresses
SSH IP Whitelist
Isolation and Killing of Malicious Programs

Alarms will not be generated for login attempts from common login IP addresses.

You can add 14 more common login IP addresses.

Add Common Login IP Address
Select a property or enter a keyword.

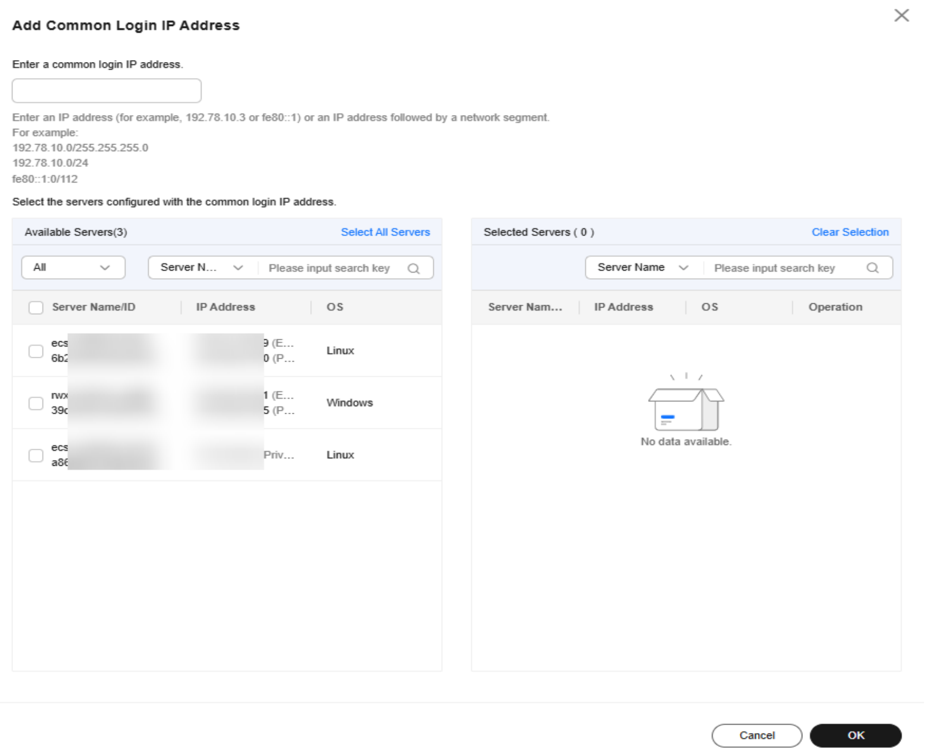
| Common Login IP Addresses | Server Quantity | Operation |
|---|---|---|

3. In the dialog box that is displayed, enter a common login IP address and select servers. Confirm the information and click **OK**.

   NOTE

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

**Figure 6-5** Entering a common login IP address



Add Common Login IP Address

Enter a common login IP address.

Enter an IP address (for example, 192.78.10.3 or fe80::1) or an IP address followed by a network segment.
For example:
192.78.10.0/255.255.255.0
192.78.10.0/24
fe80::1:0/112

Select the servers configured with the common login IP address.

Available Servers(3) Select All Servers

| □ Server Name/ID | IP Address | OS |
|---|---|---|
| □ ecs [redacted]<br>6b2 [redacted] | [redacted] 9 (E...<br>0 (P... | Linux |
| □ rwx [redacted]<br>39c [redacted] | [redacted] 1 (E...<br>5 (P... | Windows |
| □ ecs [redacted]<br>a86 [redacted] | [redacted] Priv... | Linux |

Selected Servers ( 0 ) Clear Selection

| Server Nam... | IP Address | OS | Operation |
|---|---|---|---|

No data available.

4. Return to the Common Login IP Addresses sub-tab and check the added common login IP addresses.

**Step 6 Configuring an SSH login IP address whitelist**

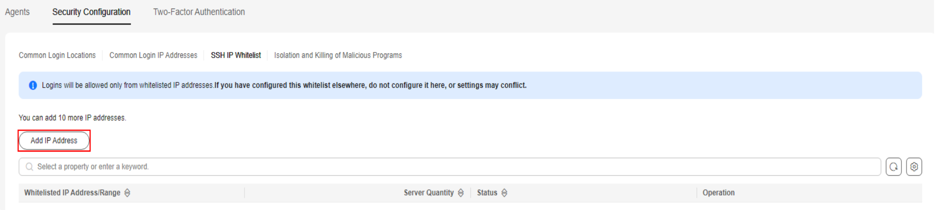
NOTE

- 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.

1. Choose **Security Configuration** > **SSH IP Whitelist**. The **SSH IP Whitelist** page is displayed.
2. Click **Add IP Address**. The **Add IP Address** dialog box is displayed.

**Figure 6-6** Configuring an IP address whitelist



Agents | Security Configuration | Two-Factor Authentication

Common Login Locations | Common Login IP Addresses | SSH IP Whitelist | Isolation and Killing of Malicious Programs

Logins will be allowed only from whitelisted IP addresses.**If you have configured this whitelist elsewhere, do not configure it here, or settings may conflict.**

You can add 10 more IP addresses.

Add IP Address

Select a property or enter a keyword.

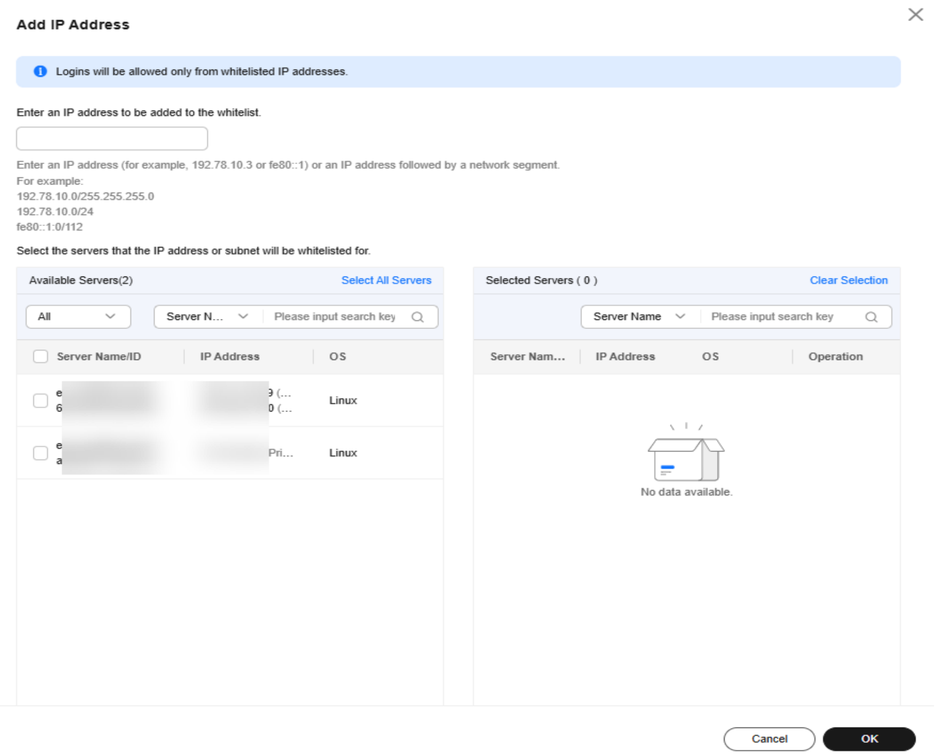
| Whitelisted IP Address/Range | Server Quantity | Status | Operation |
|---|---|---|---|

3. In the dialog box that is displayed, enter an IP address to be added to the whitelist and select servers. Confirm the information and click **OK**.

   NOTE

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

**Figure 6-7** Entering an IP address



**Add IP Address**

Logins will be allowed only from whitelisted IP addresses.

Enter an IP address to be added to the whitelist.

Enter an IP address (for example, 192.78.10.3 or fe80::1) or an IP address followed by a network segment.
For example:
192.78.10.0/255.255.255.0
192.78.10.0/24
fe80::1:0/112

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

Available Servers(2) | Select All Servers

All | Server N... | Please input search key

| Server Name/ID | IP Address | OS |
|---|---|---|
| □ e [redacted] 6 [redacted] | [redacted] 9 (...<br>0 (... | Linux |
| □ e [redacted] a [redacted] | [redacted] Pri... | Linux |

Selected Servers ( 0 ) | Clear Selection

Server Name | Please input search key

| Server Nam... | IP Address | OS | Operation |
|---|---|---|---|

No data available.

Cancel | OK

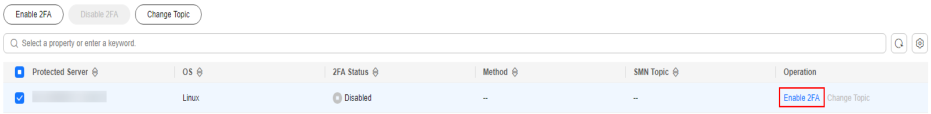
4. The **SSH IP Whitelist** sub-tab and check the added IP whitelist.

**Step 7** **Configuring 2FA**

1. Choose **Two-Factor Authentication** tab. The **Two-Factor Authentication** page is displayed.
2. Click **Enable 2FA** in the **Operation** column of the target server. The **Enable 2FA** dialog box is displayed.

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

**Figure 6-8** Enabling 2FA



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

3. In the dialog box, select the authentication mode.

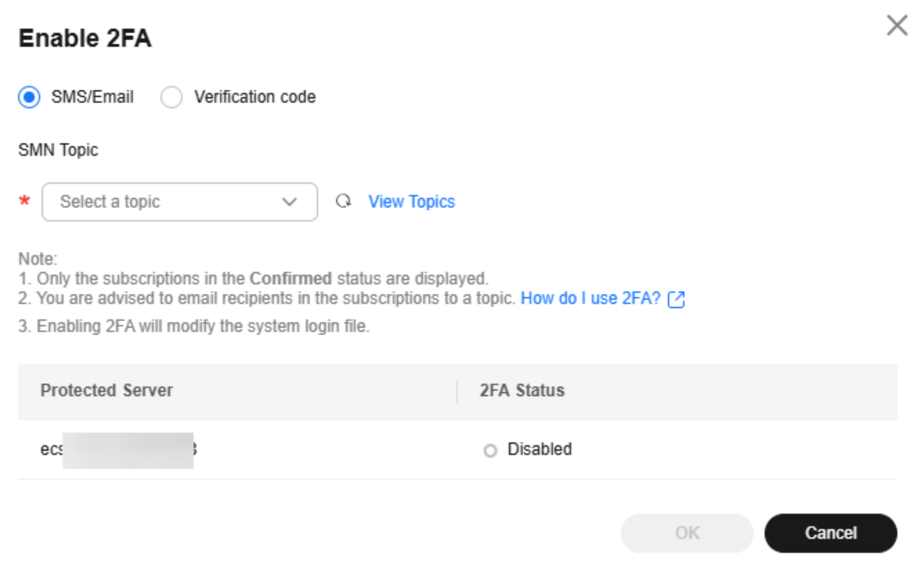
   – **SMS/Email**

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

     - The drop-down list displays only notification topics that have been confirmed.
     - If there is no topic, click **View** to create one. For details, see **Creating a Topic**.
     - If your topic contains multiple mobile numbers or email addresses, during two-factor authentication,
       - If you use a mobile phone number for verification, all the endpoints (mobile numbers and email addresses) in the topic will receive a verification code.
       - If you use an email address for verification, only this address will receive a verification code.

       You can delete the mobile numbers and email addresses that do not need to receive verification messages.

     **Figure 6-9** SMS/Email verification



**Enable 2FA**

● SMS/Email ○ Verification code

SMN Topic

* Select a topic View Topics

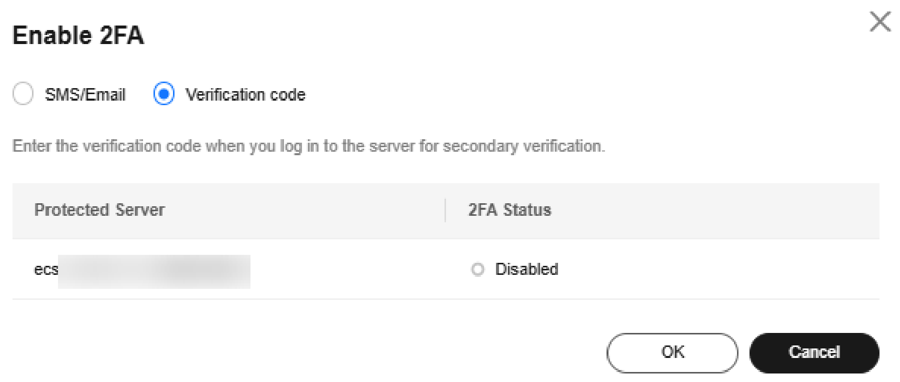
Note:
1. Only the subscriptions in the Confirmed status are displayed.
2. You are advised to email recipients in the subscriptions to a topic. How do I use 2FA?
3. Enabling 2FA will modify the system login file.

| Protected Server | 2FA Status |
|---|---|
| ecs[redacted] | Disabled |

   – **Verification code**

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

**Figure 6-10** Setting Method to Verification code



Enable 2FA

○ SMS/Email ● Verification code

Enter the verification code when you log in to the server for secondary verification.

| Protected Server | 2FA Status |
|---|---|
| ecs[redacted] | ○ Disabled |

4. Click **OK**.
5. Return to the **Two-Factor Authentication** tab. 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.

**Step 8 Configuring weak password detection**

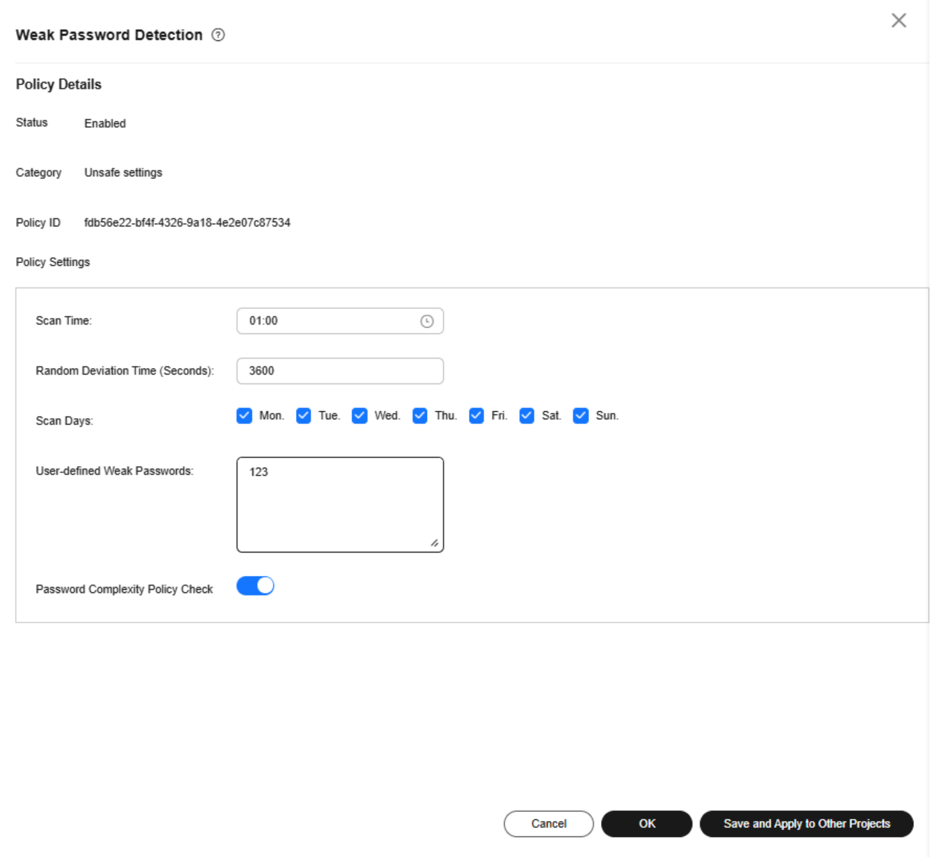
1. In the navigation pane, choose **Security Operations** > **Policies**.
2. Click the name of the target policy group. The policy list page is displayed.

   You can determine the OS and protection version supported by the target policy based on its default policy group description and supported version.

   NOTE

   If you need to create a policy group, perform this step after **Creating a Policy Group**.
3. Click the **Weak Password Detection**. The **Weak Password Detection** dialog box is displayed.
4. Modify the parameters in the **Policy Settings** based on the site requirements. For details about the parameters, see **Table 6-1**.

**Figure 6-11** Modifying the weak password detection policy



Weak Password Detection

Policy Details

Status Enabled

Category Unsafe settings

Policy ID fdb56e22-bf4f-4326-9a18-4e2e07c87534

Policy Settings

Scan Time: 01:00

Random Deviation Time (Seconds): 3600

Scan Days: ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. ☑ Sat. ☑ Sun.

User-defined Weak Passwords: 123

Password Complexity Policy Check ●

**Table 6-1** Parameter description

| Parameter | Description | Example Value |
|---|---|---|
| Scan Time | Time point when detections are performed. It can be accurate to the minute. | 01:00 |
| Random Deviation Time (Seconds) | Random deviation time of the weak password based on **Scan Time**. The value range is 0 to 7200s. | 3600 |
| Scan Days | Days in a week when weak passwords are scanned. You can select one or more days. | Select all of them. |
| 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.<br>Enter only one weak password per line. Up to 300 weak passwords can be added. | test123* |

| Parameter | Description | Example Value |
|---|---|---|
| Password Complexity Policy Check | A password complexity policy refers to the password rules and standards set on a server. If you enable **Password Complexity Policy Check**, HSS will check the password complexity policy when you manually perform a baseline check. | ● |

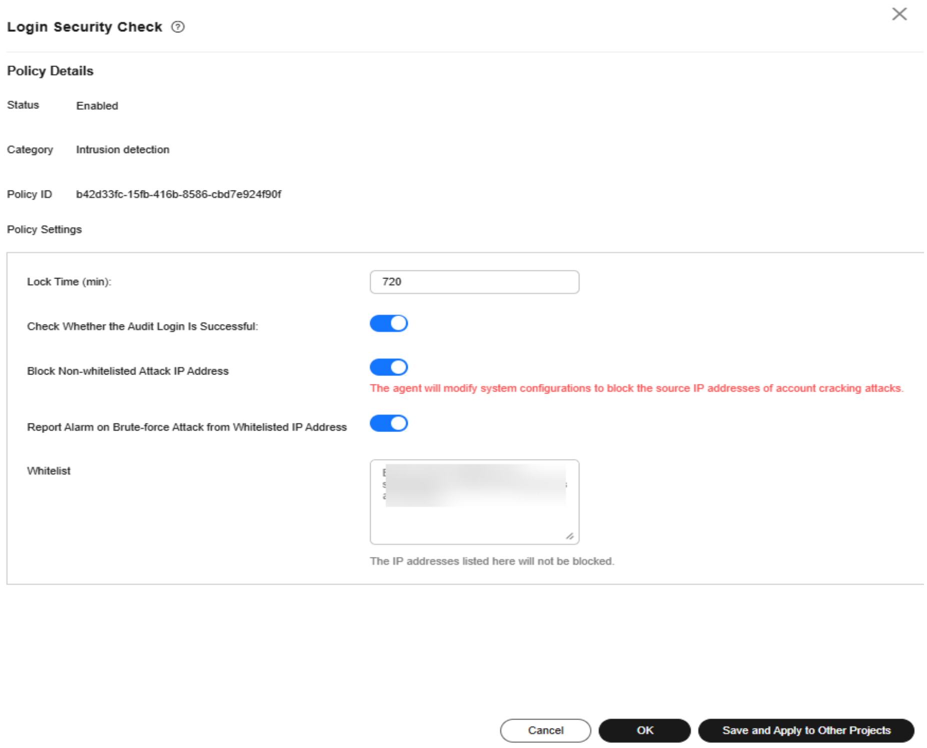
5. Confirm the information and click **OK**.

   HSS will perform weak password detection on the server based on the configured policies.

**Step 9** **Configuring login security check**

1. Click **Login Security Check**. The **Login Security Check** dialog box is displayed.
2. Modify the parameters in the **Policy Settings** based on the site requirements. For details about the parameters, see **Table 6-2**.

**Figure 6-12** Modifying the security check policy



Login Security Check

Policy Details

Status Enabled

Category Intrusion detection

Policy ID b42d33fc-15fb-416b-8586-cbd7e924f90f

Policy Settings

Lock Time (min): 720

Check Whether the Audit Login Is Successful: ●

Block Non-whitelisted Attack IP Address ●

The agent will modify system configurations to block the source IP addresses of account cracking attacks.

Report Alarm on Brute-force Attack from Whitelisted IP Address ●

Whitelist

The IP addresses listed here will not be blocked.

**Table 6-2** 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. |
| Check Whether the Audit Login Is Successful | – After this function is enabled, HSS reports login success logs.<br>▪ ●: enabled<br>▪ ○: 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.<br>▪ ●: enabled<br>▪ ○: 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. |

3. Confirm the information and click **OK**.

   HSS will perform login security detection on the server based on the configured policies.

**----End**

# 7 Using HSS and CBR to Defend Against Ransomware

## 7.1 Overview

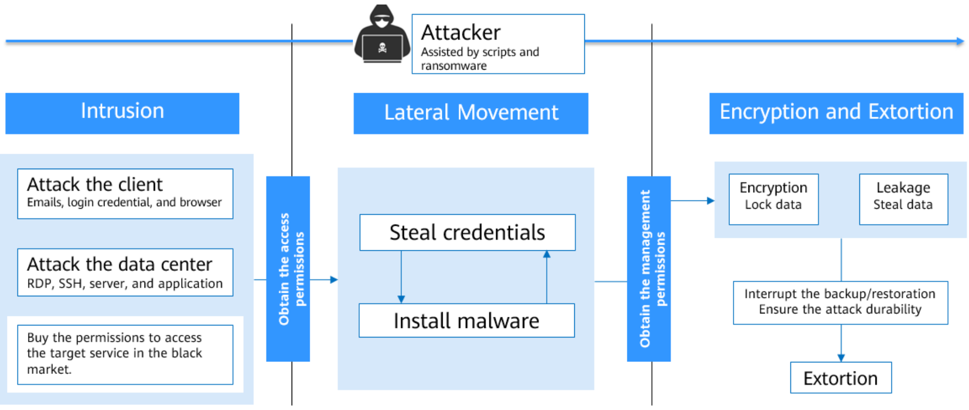
### Scenario

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.

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 7-1** Extortion process


Attacker
Assisted by scripts and ransomware
Intrusion
Attack the client
Emails, login credential, and browser
Attack the data center
RDP, SSH, server, and application
Buy the permissions to access the target service in the black market.
Obtain the access permissions
Lateral Movement
Steal credentials
Install malware
Obtain the management permissions
Encryption and Extortion
Encryption
Lock data
Leakage
Steal data
Interrupt the backup/restoration
Ensure the attack durability
Extortion

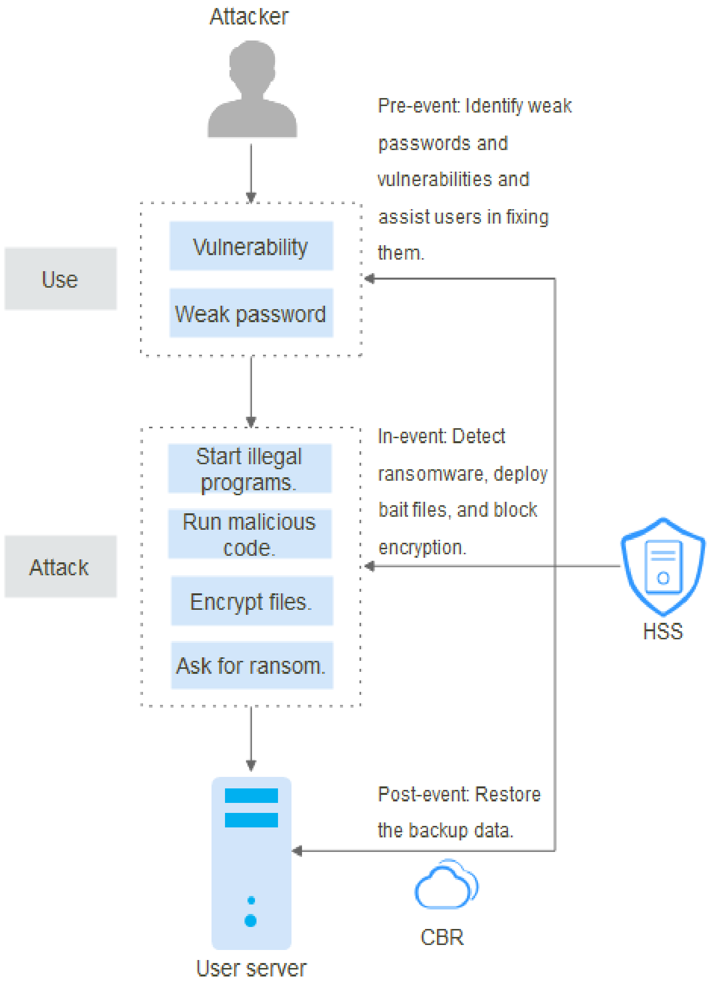
This solution describes how to use HSS and CBR to implement three-phase protection for servers, including pre-event prevention, in-event detection and timely blocking, and post-event backup and restoration.

## Architecture

Enterprises or individuals can use HSS to detect ransomware and identify system risks. CBR can be used to back up service data and plan and control account permissions and organizational structures.

The following figure **HSS+CBR ransomware protection** shows the protection principle.

**Figure 7-2** HSS+CBR ransomware protection


Attacker
Pre-event: Identify weak passwords and vulnerabilities and assist users in fixing them.
Use
Vulnerability
Weak password
In-event: Detect ransomware, deploy bait files, and block encryption.
Attack
Start illegal programs.
Run malicious code.
Encrypt files.
Ask for ransom.
HSS
Post-event: Restore the backup data.
CBR
User server

For details about the defense measures in the figure, see:

- Pre-event: Identify weak passwords and vulnerabilities and assist users in fixing them.

  For details, see **Identifying and Fixing Ransomware**.
- In-event: Detect ransomware, deploy bait files, and block encryption.

  For details, see **Enabling Ransomware Prevention and Backup**.
- Post-event: Restore the backup data.

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

## Advantages

- Reduce system risks.

  Users can use HSS to periodically detect vulnerabilities and risks in the system and rectify them in a timely manner.
- Detect and block ransomware attacks in real time.

After ransomware protection is enabled, HSS detects ransomware attacks in real time, generates alarms, and isolates ransomware programs.

- Back up service data to enhance anti-risk capabilities.

  If a server is attacked by ransomware, CBR can be used to restore backup data and services in a timely manner and reduce losses.

# 7.2 Resources and Costs

The following table describes the resource planning in the best practice.

**Table 7-1** Resource description

| Resource | Description | Cost |
|---|---|---|
| HSS (Host Security Service) | One HSS premium edition quota. One HSS premium edition quota is required to protect one server. | For details about billing rules, see **Billing Description**. |
| Cloud Backup and Recovery (CBR) | One ECS backup vault. | For details about billing rules, see **Billing Description**. |

# 7.3 Defense Measures

## 7.3.1 Identifying and Fixing Ransomware

According to the Huawei Cloud statistics on security intrusion events, 90% of ransomware attacks result from weak passwords, vulnerability exploits, and unsafe baseline settings. Identifying and fixing risks before real intrusions can significantly improve the system security. Huawei Cloud HSS helps you quickly identify risks and provides the one-click fix function to reduce 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.

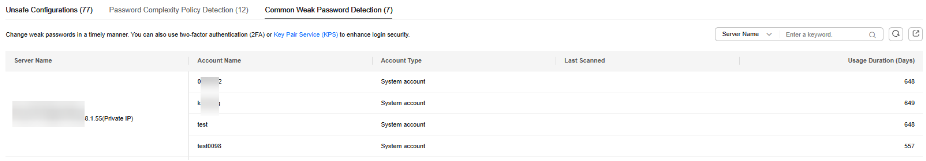
**Step 1** **Log in to the management console**.

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

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

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

**Figure 7-3** Viewing common weak password detection



Unsafe Configurations (77)
Password Complexity Policy Detection (12)
Common Weak Password Detection (7)
Server Name
Enter a keyword.

Change weak passwords in a timely manner. You can also use two-factor authentication (2FA) or Key Pair Service (KPS) to enhance login security.

| Server Name | Account Name | Account Type | Last Scanned | Usage Duration (Days) |
|---|---|---|---|---|
| [redacted]8.1.55(Private IP) | 0[redacted]2 | System account |  | 648 |
|  | k[redacted] | System account |  | 649 |
|  | test | System account |  | 648 |
|  | test0098 | System account |  | 557 |

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

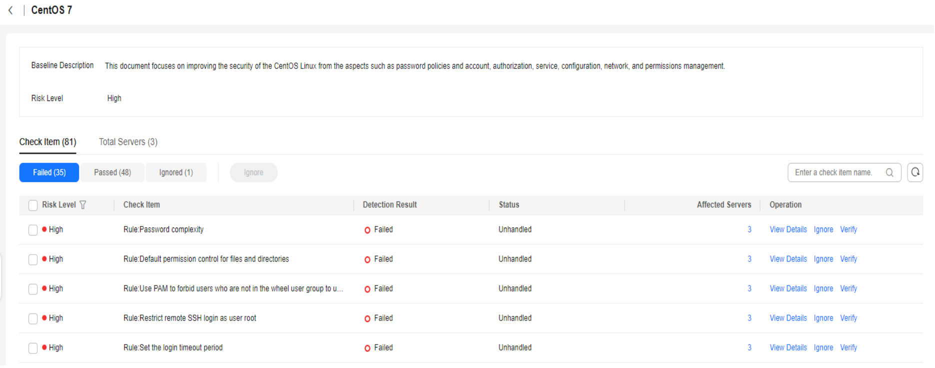
**Step 3** In the navigation pane on the left, choose **Risk Management** > **Baseline Checks**.

**Step 4** Click the **Unsafe Configurations** tab to view the unsafe configurations of the server.

**Step 5** Click the target baseline name. The baseline details page is displayed.

**Step 6** Click the **Check Items** tab and click **Failed** to view baseline risk items.

**Figure 7-4** Viewing baseline check details



Baseline Description This document focuses on improving the security of the CentOS Linux from the aspects such as password policies and account, authorization, service, configuration, network, and permissions management.

Risk Level High

| Risk Level | Check Item | Detection Result | Status | Affected Servers | Operation |
|---|---|---|---|---|---|
| ● High | Rule:Password complexity | ○ Failed | Unhandled | 3 | View Details Ignore Verify |
| ● High | Rule:Default permission control for files and directories | ○ Failed | Unhandled | 3 | View Details Ignore Verify |
| ● High | Rule:Use PAM to forbid users who are not in the wheel user group to u... | ○ Failed | Unhandled | 3 | View Details Ignore Verify |
| ● High | Rule:Restrict remote SSH login as user root | ○ Failed | Unhandled | 3 | View Details Ignore Verify |
| ● High | Rule:Set the login timeout period | ○ Failed | Unhandled | 3 | View Details Ignore Verify |

**Step 7** Click **View Details** in the **Operation** column of a check item to view the modification suggestions and affected servers.

**Step 8** Log in to the affected server and harden the configuration based on the modification suggestions.

**Step 9** 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 **Automatic Vulnerability Scan**.

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

**Step 3** In the navigation pane on the left, choose **Risk Management** > **Vulnerabilities**. The vulnerability management page is displayed.

**Step 4** Click the **Linux Vulnerabilities**, **Windows Vulnerabilities**, **Web-CMS Vulnerabilities**, **Application Vulnerabilities**, and **Emergency Vulnerabilities** tabs to view the vulnerabilities of the server.

**Step 5** 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, application, and emergency 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.

     For details, see **Creating a CSBS Backup**.

  2) Fix vulnerabilities on the current server.

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

  NOTE

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

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**

## 7.3.2 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 is an anti-intrusion, anti-encryption, and anti-proliferation ransomware detection engine that uses the dynamic deception technology. HSS can scan and kill 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: Creating a Ransomware Prevention Policy

Create a ransomware prevention policy and configure honeypot file directories, excluded directories, and protected file types based on service requirements.

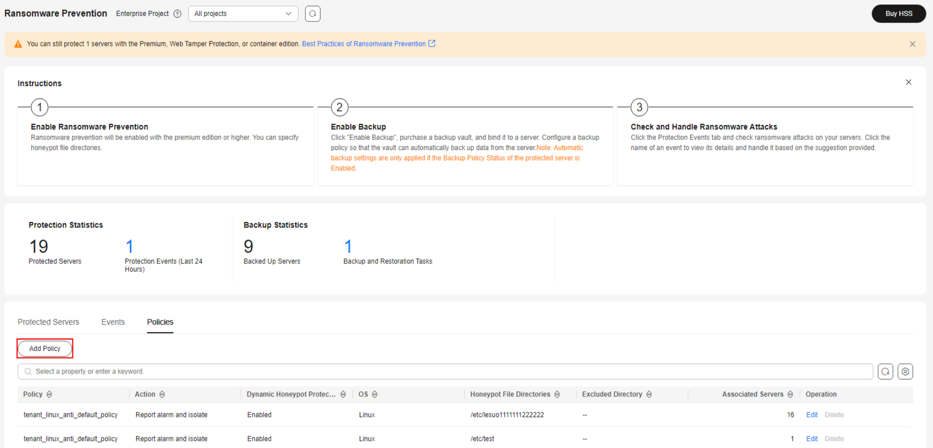
**Step 1** **Log in to the management console**.

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

**Step 3** Choose **Server Protection** > **Ransomware Prevention**.

**Step 4** Click the **Policies** tab. Click **Add Policy**. The **Add Policy** dialog box is displayed.

**Figure 7-5** Adding a protection policy



You can still protect 1 servers with the Premium, Web Tamper Protection, or container edition. Best Practices of Ransomware Prevention

**Enable Ransomware Prevention**
Ransomware prevention will be enabled with the premium edition or higher. You can specify honeypot file directories.

**Enable Backup**
Click "Enable Backup", purchase a backup vault, and bind it to a server. Configure a backup policy so that the vault can automatically back up data from the server.Note: Automatic backup settings are only applied if the Backup Policy Status of the protected server is Enabled.

**Check and Handle Ransomware Attacks**
Click the Protection Events tab and check ransomware attacks on your servers. Click the name of an event to view its details and handle it based on the suggestion provided.

19 Protected Servers

1 Protection Events (Last 24 Hours)

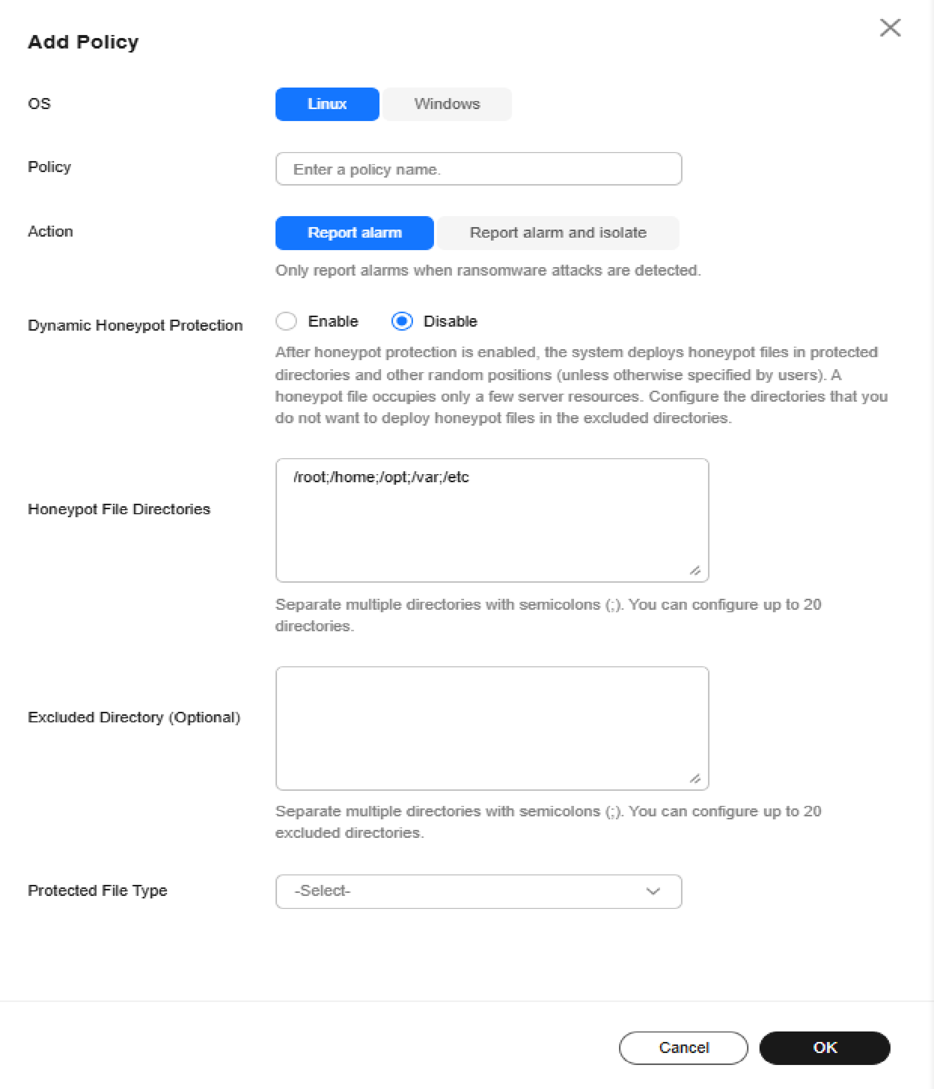
9 Backed Up Servers

1 Backup and Restoration Tasks

| Policy | Action | Dynamic Honeypot Protec... | OS | Honeypot File Directories | Excluded Directory | Associated Servers | Operation |
|---|---|---|---|---|---|---|---|
| tenant_linux_anti_default_policy | Report alarm and isolate | Enabled | Linux | /etc/lesuo1111111222222 | -- | 16 | Edit Delete |
| tenant_linux_anti_default_policy | Report alarm and isolate | Enabled | Linux | /etc/test | -- | 1 | Edit Delete |

**Step 5** Configure the policy information by referring to **Table 7-2**.

**Figure 7-6** Protection policy parameters



Add Policy

OS: Linux | Windows

Policy: Enter a policy name.

Action: Report alarm | Report alarm and isolate

Only report alarms when ransomware attacks are detected.

Dynamic Honeypot Protection: ○ Enable ● Disable

After honeypot protection is enabled, the system deploys honeypot files in protected directories and other random positions (unless otherwise specified by users). A honeypot file occupies only a few server resources. Configure the directories that you do not want to deploy honeypot files in the excluded directories.

Honeypot File Directories: /root;/home;/opt;/var;/etc

Separate multiple directories with semicolons (;). You can configure up to 20 directories.

Excluded Directory (Optional):

Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.

Protected File Type: -Select-

**Table 7-2** Protection policy parameters

| Parameter | Description | Example Value |
|---|---|---|
| OS | Server OS. | Linux |
| Policy | Policy name | test |
| Action | Indicates how an event is handled.<br>● **Report alarm and isolate**<br>● **Report alarm** | **Report alarm and isolate** |

| Parameter | Description | Example Value |
|---|---|---|
| Dynamic Honeypot Protection | After honeypot protection is enabled, the system deploys honeypot files in protected directories and other random locations (unless otherwise specified by users). The honeypot files deployed in random locations are automatically deleted every 12 hours and then randomly deployed again. A honeypot file occupies a few server resources. Therefore, configure the directories that you do not want to deploy the honeypot file in the excluded directories.<br>**NOTE**<br>Currently, Linux servers support dynamic generation and deployment of honeypot files. Windows servers support only static deployment of honeypot files. | Enable |
| Honeypot File Directories | Directory that needs to be protected by static honeypot (excluding subdirectories). You are advised to configure important service directories or data directories.<br>Separate multiple directories with semicolons (;). You can configure up to 20 directories.<br>This parameter is mandatory for Linux servers and optional for Windows servers. | Linux: **/etc**<br>Windows: **C:\Test** |
| Excluded Directory (Optional) | Directory that does not need to be protected by honeypot files.<br>Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories. | Linux: **/etc/lesuo**<br>Windows: **C:\Test \ProData** |
| File Type | Types of files to be protected.<br>More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups.<br>This parameter is mandatory for Linux servers only. | Select all |

| Parameter | Description | Example Value |
|---|---|---|
| (Optional) Process Whitelist | Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms.<br>This parameter is mandatory only for Windows servers. | - |

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

**----End**

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

**Step 3** Choose **Server Protection** > **Ransomware Prevention**.

**Step 4** Click the **Protected Servers** tab.

**Step 5** Select the target server and click **Enable Ransomware Prevention** above the list.

**Step 6** In the **Enable Ransomware Prevention** dialog box, confirm the server information and select a protection policy.

**Step 7** Click **OK**.

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

**----End**

## 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 **Purchasing a Server Backup Vault** and then enable the backup function.

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

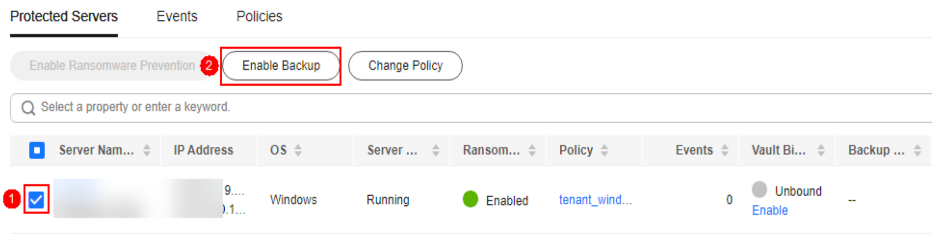
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

**Step 3** Choose **Server Protection** > **Ransomware Prevention**.

**Step 4** Click the **Protected Servers** tab.

**Step 5** Select a server and click **Enable Backup** in the upper part of the server list.

**Figure 7-7** Enabling backup


Protected Servers
Events
Policies
Enable Ransomware Prevention
2
Enable Backup
Change Policy
Select a property or enter a keyword.
1

| ■ | Server Nam... | IP Address | OS | Server ... | Ransom... | Policy | Events | Vault Bi... | Backup ... |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | [redacted] | [redacted] 9....<br>.1... | Windows | Running | ● Enabled | tenant_wind... | 0 | ● Unbound<br>Enable | -- |

**Step 6** In the **Enable Backup** dialog box, select a vault.

NOTE

A vault that meets the following conditions can be bound:

- The vault is in **Available** or **Locked** state.
- The backup policy is in **Enabled** state.
- The vault has backup capacity available.
- The vault is bound to fewer than 256 servers.

**Step 7** Click **OK**.

**----End**

## Step 4: Handling the Alarm and Isolate the Infected Device.

When an intruder bypasses the defense mechanism, if you can detect and block the intruder in a timely manner, a disaster can be avoided. When enabling ransomware protection, you need to handle intrusion alarms in a timely manner to prevent ransomware from running and spreading.

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

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

**Step 3** In the navigation tree on the left, choose **Server Protection > Ransomware Prevention**.

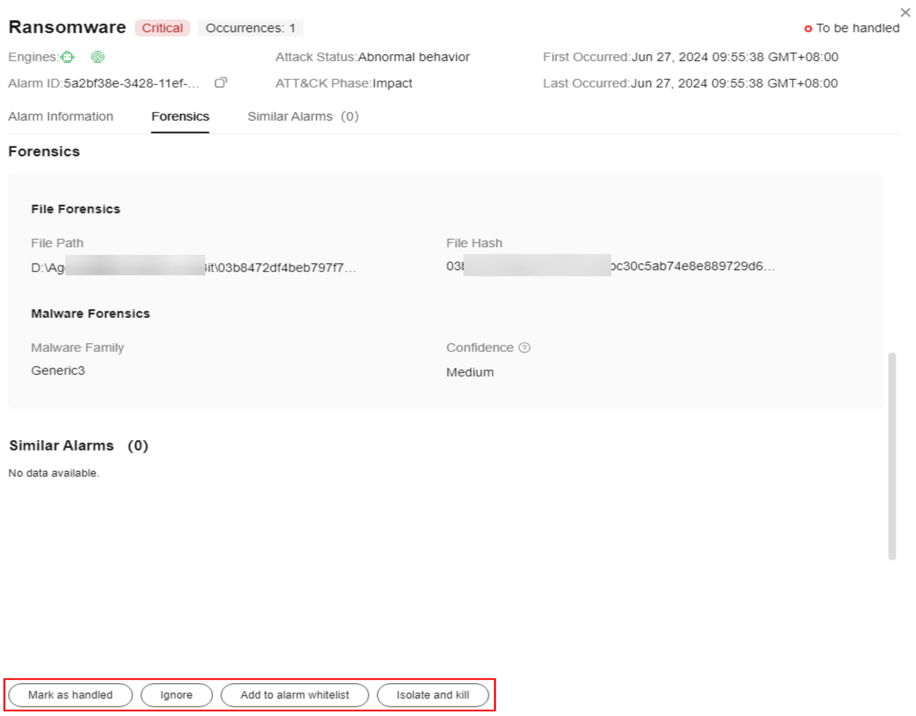
**Step 4** Click the **Events** tab to view ransomware alarms.

**Step 5** Click an alarm name to view its details.

You can check whether ransomware exists on the server based on alarms and forensics.

**Step 6** Select an alarm handling mode at the bottom of the page.

**Figure 7-8** Selecting an alarm handling mode



Ransomware Critical Occurrences: 1 ○ To be handled

Engines:

Attack Status:Abnormal behavior

First Occurred:Jun 27, 2024 09:55:38 GMT+08:00

Alarm ID:5a2bf38e-3428-11ef-...

ATT&CK Phase:Impact

Last Occurred:Jun 27, 2024 09:55:38 GMT+08:00

Forensics

File Forensics

File Path: D:\Ag[redacted]it\03b8472df4beb797f7...

File Hash: 03[redacted]bc30c5ab74e8e889729d6...

Malware Forensics

Malware Family: Generic3

Confidence: Medium

Similar Alarms (0)

No data available.

- **Mark as handled**: If you have handled the event manually, you can choose **Mark as handled**.
- **Ignore**: If an alarm does not need to be handled, you can choose **Ignore**. After the alarm is ignored, the alarm status changes to **Handled**. HSS will not collect statistics on this event.
- **Add to alarm whitelist**: If an alarm is falsely reported, you can select **Add to alarm whitelist**. HSS will not report alarms later.
- **Isolate and kill**: If the alarm is caused by a ransomware program, you can select **Isolate and kill**. After the isolation, the program cannot perform **read/write** operations, and the process of the program is terminated immediately.

CAUTION

Once being attacked, immediately disconnect the network or power off the system to prevent the spread of the ransomware attack. In addition, change the passwords of infected devices and other devices on the same LAN in a timely manner.

**Step 7** In the **Handle Event** dialog box, click **OK**.

**----End**

## Related Operations

Besides using HSS and CBR, you are advised to use the following methods to improve **anti-attack capabilities**.

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

## 7.3.3 Restoring Backup Data

Ransomware attacks are developing rapidly these days. There are no tools can kill them absolutely. So once a system was attacked by ransomware, restoring the victim system from backups in a timely manner is the best remedies to minimize losses. After enabling ransomware backup, you can use Huawei Cloud CBR to quickly restore services, keeping your services stable.

### Restoring Backup Data

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.

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

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

**Step 3** In the navigation tree on the left, choose **Server Protection > Ransomware Prevention**.

**Step 4** Click the **Protected Servers** tab.

**Step 5** In the **Operation** column of the target server, click **More** > **Restore Data**.

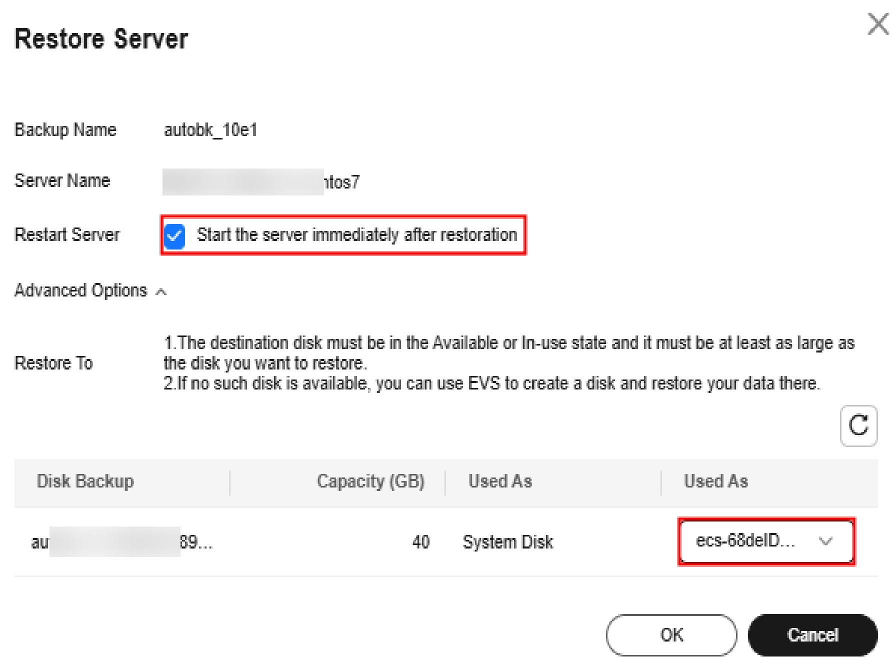
**Step 6** In the displayed **Backups** page, select the backup data you want to restore.

**Step 7** In the **Operation** column of the target backup data, click **Restore Data**.

**Step 8** In the displayed dialog page, confirm the server information and configure parameters such as the disk for storing data.

- **Restart Server**: If this option is selected, you agree to restart the server after data restoration.
- **Advanced Options**: Click ⌄ to expand it. Select the location where the backup data is restored.

**Figure 7-9** Restoring a server



Restore Server

Backup Name autobk_10e1

Server Name [redacted]tos7

Restart Server ☑ Start the server immediately after restoration

Advanced Options ^

Restore To 1.The destination disk must be in the Available or In-use state and it must be at least as large as the disk you want to restore.
2.If no such disk is available, you can use EVS to create a disk and restore your data there.

| Disk Backup | Capacity (GB) | Used As | Used As |
|---|---|---|---|
| au[redacted]89... | 40 | System Disk | ecs-68delD... ⌄ |

**Step 9** Click **OK**.

**----End**

## Related Operations

You are advised to identify system vulnerabilities based on the ransomware attack path and fix system vulnerabilities.

# 8 Using HSS to Scan and Fix Vulnerabilities

## Scenario

HSS can scan for Linux, Windows, Web-CMS, application, and emergency vulnerabilities and provide multiple vulnerability handling methods, helping you comprehensively understand and fix vulnerabilities in your assets in a timely manner and avoid potential risks.

You can discover and fix vulnerabilities using HSS.

## Prerequisites

HSS Professional, Enterprise, Premium, Web Tamper Protection, or Container Edition has been enabled for the server. For details, see **HSS Access Overview**.

## Determining the Urgency for Fixing the Vulnerability

If multiple vulnerabilities are detected in your assets, you can use the following methods to determine the urgency of the vulnerabilities and fix the vulnerabilities that have significant impact on your server first.

- Determined by **vulnerability fixing priority**

  You can fix vulnerabilities based on their priorities. Generally, vulnerabilities whose **Priority** is **Critical** must be fixed immediately.

  The vulnerability fix priority is weighted based on the CVSS score, release time, and the importance of the assets affected by the vulnerability. It reflects the urgency of the fix.

  NOTE

  By default, the importance of an asset is **General**. You can also change it. For details, see **Servers Importance Management** .

  Vulnerabilities are classified into four priority levels: critical, high, medium, and low. You can refer to the priorities to fix the vulnerabilities that have significant impact on your server first.

  - **Critical**: This vulnerability must be fixed immediately. Attackers may exploit this vulnerability to cause great damage to the server.

  - **High**: This vulnerability must be fixed as soon as possible. Attackers may exploit this vulnerability to damage the server.
  - **Medium**: You are advised to fix the vulnerability to enhance your server security.
  - **Low**: This vulnerability has a small threat to server security. You can choose to fix or ignore it.
- Determined based on **actual business conditions**.

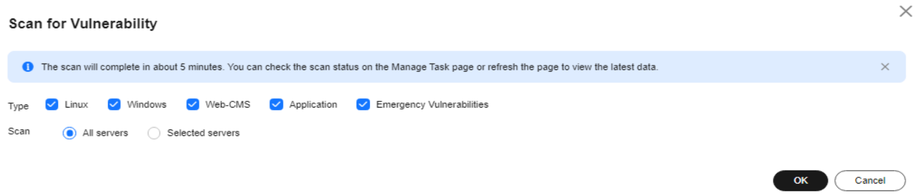
  You can view vulnerability details and determine whether to fix vulnerabilities as soon as possible based on actual services and affected servers.

## Scanning for and Fixing Vulnerabilities

**Step 1** **Scan for vulnerabilities.**

1. **Log in to the management console**.
2. In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.
3. In the navigation pane, Choose **Risk Management** > **Vulnerabilities**.
4. In the upper right corner of the **Vulnerabilities** page, click **Scan**.
5. In the displayed **Scan for Vulnerability** dialog box, select all **Type** and set **Scan** to **All servers** to ensure that all possible vulnerabilities of all servers can be scanned.

   **Figure 8-1** Setting manual scan parameters

   Scan for Vulnerability

   The scan will complete in about 5 minutes. You can check the scan status on the Manage Task page or refresh the page to view the latest data.

   Type ☑ Linux ☑ Windows ☑ Web-CMS ☑ Application ☑ Emergency Vulnerabilities

   Scan ● All servers ○ Selected servers

6. In the upper right corner of the **Vulnerabilities** page, click **Manage Task**. On the **Scan Tasks** tab page, confirm that the manual scan task has been completed and ensure that the detected vulnerability information is updated immediately.

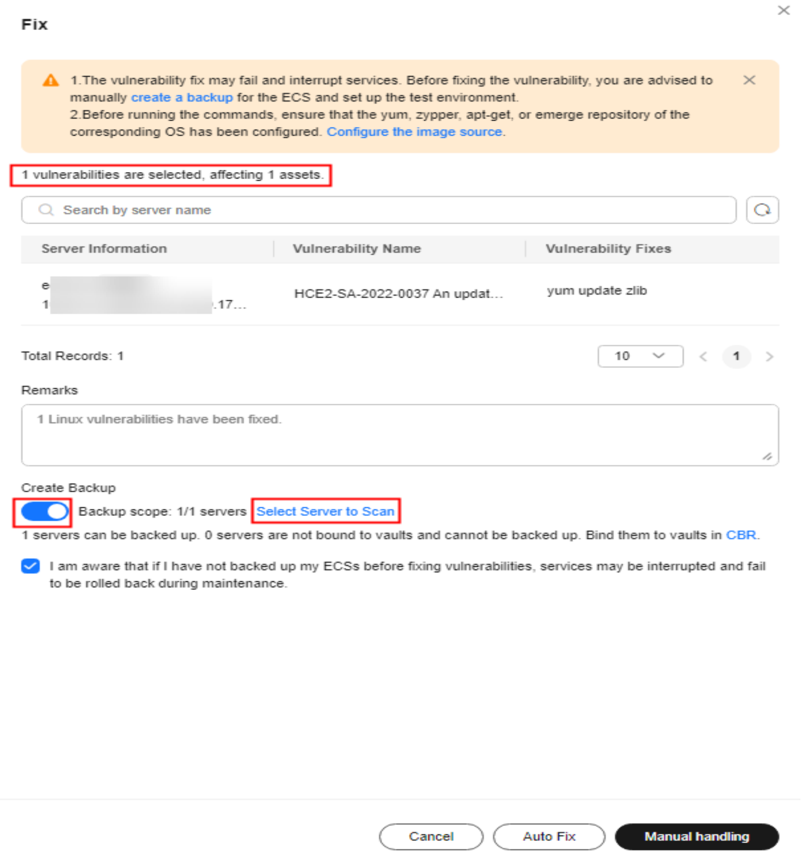
**Step 2** **Fix vulnerabilities.**

**⚠ CAUTION**

- Vulnerability fixing operations cannot be rolled back. If a vulnerability fails to be fixed, services will probably be interrupted, and incompatibility issues will probably occur in middleware or upper layer applications. To prevent unexpected consequences, you are advised to use CBR to back up ECSs. For details, see **Purchasing a Server Backup Vault**. Then, use idle servers to simulate the production environment and test-fix the vulnerability. If the test-fix succeeds, fix the vulnerability on servers running in the production environment.
- Servers need to access the Internet and use external image sources to fix vulnerabilities.
  - Linux OS: If your servers cannot access the Internet, or the external image sources cannot provide stable services, you can use the image source provided by Huawei Cloud to fix vulnerabilities. Before fixing vulnerabilities online, configure the Huawei Cloud image sources that match your server OSs. For details, see **Image Source Management**.
  - Windows OS: If your servers cannot access the Internet, ensure you have set up a patch server.

1. Filter the vulnerabilities to be fixed.
   - Click the number next to **Critical Vulnerabilities** to filter the critical vulnerabilities.
   - In the scanned vulnerability list, filter out the vulnerabilities with high priorities. For example, in the **Vulnerability view** tab, set priority to **Critical** and **High**. In the **Server view** tab, set risk level to **High** and **Medium**.
2. Fix the vulnerabilities.
   - **Auto fix**: Only Linux and Windows vulnerabilities can be automatically fixed. The following example describes how to fix a Linux vulnerability.
     i. On the **Vulnerabilities** page, click **Fix** in the **Operation** column of the target vulnerability.
     ii. In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets, and click ○ to enable backup.

**Figure 8-2** Confirming vulnerabilities and creating backups



Fix

1.The vulnerability fix may fail and interrupt services. Before fixing the vulnerability, you are advised to manually create a backup for the ECS and set up the test environment.
2.Before running the commands, ensure that the yum, zypper, apt-get, or emerge repository of the corresponding OS has been configured. Configure the image source.

1 vulnerabilities are selected, affecting 1 assets.

Search by server name

| Server Information | Vulnerability Name | Vulnerability Fixes |
|---|---|---|
| e [redacted]<br>1 [redacted] .17... | HCE2-SA-2022-0037 An updat... | yum update zlib |

Total Records: 1

Remarks

1 Linux vulnerabilities have been fixed.

Create Backup

Backup scope: 1/1 servers Select Server to Scan

1 servers can be backed up. 0 servers are not bound to vaults and cannot be backed up. Bind them to vaults in CBR.

☑ I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.

iii. Click **Select Server to Scan**. In the **Create Backup** dialog box, set the **Backup Name** and click **OK**.

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

v. Click the vulnerability name. On the details page, click the **Handling History** tab and view the vulnerability fixing status in the **Status** column of the target vulnerability.

- **Fixed** indicates that the vulnerability has been successfully fixed. For details, see **Vulnerability fix statuses**.
- **Failed** indicates that the vulnerability fails to be fixed. The possible cause is that the vulnerability does not exist or has been changed. You can view the cause of the vulnerability fixing failure and fix the vulnerability by referring to the methods provided by HSS. For details, see **What Do I Do If Vulnerability Fix Failed?**

– **Manually handling**: Web-CMS vulnerabilities, application vulnerabilities, and emergency vulnerabilities cannot be automatically fixed. You need to manually fix them by referring to the methods.

i. On the **Vulnerabilities** page, click the name of the target vulnerability. On the details page, view the fixing suggestions.

ii. Select a solution to fix the vulnerability based on the service requirements.

**Method 1: Create a VM to fix the vulnerability.**

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

📖 NOTE

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

– **Ignoring a vulnerability** and **whitelisting a vulnerability**

If a vulnerability is harmless, you can ignore it. If a vulnerability alarm is ignored but is triggered again in the next vulnerability scan, HSS will still report the alarm to you. If a vulnerability does not affect services, you can add it to the whitelist. After a vulnerability is added to the whitelist, the detected vulnerability will be ignored and will not be reported. In addition, the vulnerability will not be scanned. For details, see **Ignoring a Vulnerability** and **Whitelisting a Vulnerability**.

**Step 3** **Restart the server.**

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

**Step 4** **Verify the vulnerability fix.**

After you manually fix vulnerabilities, you are advised to verify the fixing result. For details, see **Verifying the Vulnerability Fix**.

**----End**

## Related Operations

- HSS allows you to view historical vulnerability handling records. You can filter the handled vulnerabilities. Click the **Vulnerability Name**. On the displayed page, click **Handling History** tab to view the handling history. For details, see **Viewing Vulnerability Handling History**.
- HSS allows you to export the vulnerability list. For details, see **Exporting the Vulnerability List**.

# 9 Using HSS to Prevent Weak Passwords

## Scenarios

A weak password is short, common, or something that could be rapidly guessed by brute force attacks. Common weak passwords include but are not limited to the following:

- Common default system passwords, such as admin, root, Tomcat, and manager.
- Only digits, only letters, or a combination of numbers and letters, for example, admin123, 123456, and abcde.
- Passwords that have special meanings and can be easily guessed by others, such as the birthday, name, and mobile number.
- Multiple system accounts use the same password.

Weak passwords in the server system may bring the following risks:

- Information leakage: Attackers can intrude accounts and obtain users' privacy information and financial data through brute force cracking or password guessing.
- System damage: Attackers crack weak passwords to intrude the system and maliciously attack the system. For example, attackers can delete important data, implant malware, and maliciously modify programs, causing the system to break down or fail to run.

HSS can detect common weak passwords set in the server system and key software, including weak passwords of MySQL, FTP, Redis, and system accounts in the Linux system and weak passwords of system accounts in the Windows system. You are advised to use HSS to detect weak passwords in the server system, improve password security, and change passwords periodically to avoid security risks.

## Prerequisites

HSS Professional, Enterprise, Premium, Web Tamper Protection, or Container Edition has been enabled for the server. For details, see **HSS Access Overview**.

## How Do I Avoid Weak Password Risks?

**Step 1 Check whether there are servers with weak passwords.**

HSS can check whether the current server has weak passwords. The procedure is as follows:

1. Configure a weak password detection policy.
   a. **Log in to the management console**.
   b. In the upper left corner of the page, select a region, click ≡, and choose **Security & Compliance** > **Host Security Service**.
   c. In the navigation pane, choose **Security Operations** > **Policies**.

      NOTE

      If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.
   d. Click the name of the policy group to access the policy detail list.

      HSS provides multiple preset policy groups. After protection is enabled for a server, the server is bound to a preset policy group by default. You can also click **Copy** in the **Operation** column of a policy group. For details, see **Creating a Custom Policy Group**.
   e. Locate the row that contains the **Weak Password Detection** policy and click enable in the **Operation** column.
   f. Click the name of a **weak password detection** policy.
   g. Customize the scan time and interval for weak password detection. For details about the parameters, see **Table 9-1**.

**Table 9-1** Parameter description

| Parameter | Description |
|---|---|
| Scan Time | Time point when detections are performed. It can be accurate to the minute. |
| Random Deviation Time (Seconds) | Random deviation time of the 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.<br>Enter only one weak password per line. Up to 300 weak passwords can be added. |

| Parameter | Description |
|---|---|
| Password Complexity Policy Check | A password complexity policy refers to the password rules and standards set on a server. If you enable **Password Complexity Policy Check**, HSS will check the password complexity policy when you manually perform a baseline check. |

h. Confirm the information and click **OK**.

   If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

2. (Optional) Deploy a policy for the server.

   If you configure a weak password policy based on a newly created custom policy group in **Step 1.1**, you need to deploy the new policy group and apply it to the target server after creating and configuring the policy group. For details, see **Deploying a Protection Policy**.

3. Check for weak passwords.

   HSS automatically performs a check for all server common weak passwords at **01:00 every day**.

   If you have customized the time and period for automatic weak password detection in **a. Configure a weak password detection policy**, HSS automatically detects common weak passwords based on the configured time and period.

4. View the weak password check result.

   a. In the navigation tree on the left, choose **Risk Management > Baseline Checks**. The **Baseline Checks** page is displayed.

      NOTE

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

   b. Click **Common Weak Password Detection** tab. In the list, you can view the existing weak passwords.

**Step 2** **Change weak passwords to enhance password security.**

Check the server, account name, account type, and usage duration of the weak password detected from the **Step 1.4**. Log in to the server and change the password. For more information, see **How Do I Set a Secure Password?**.

**Step 3** **Change the password periodically.**

You are advised to change the password every 90 days.

**----End**

## How Do I Set a Secure Password?

- **Recommended password complexity**

  To ensure password security, you are advised to set the password based on the following rules:

  - Consists of 8 to 26 characters.
  - Contains at least three of the following character types:
    - Uppercase letter
    - Lowercase letter
    - Digits
    - Special characters for Windows ECSs: ! @ $ % ^ - _ = + [ { ( ) } ] : , . / ? ~ # *
    - Special characters for Linux ECSs: ! @ $ % ^ - _ = + [ { } ] : , . / ? ~ # *
  - The password cannot contain the username or the username spelled backwards.
  - For Windows servers, the password cannot contain more than two consecutive characters of the username.
- **Common methods for changing system passwords**

| 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. |

| System | Procedure | Remarks |
|---|---|---|
| MySQL database | 1. Log in to the MySQL database.<br>2. Run the following command to check the database user password: **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: **SET PASSWORD FOR'*Username*'@'*Host*'=PASSWORD('*New_password*');**<br>4. Run the following command to refresh password settings: **flush privileges;** | None |
| Redis database | 1. Open the Redis database configuration file **redis.conf**.<br>2. Run the following command to change the password: **requirepass *<password>*;** | ● If there is already a password, the command will change it to the new password.<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 |

# 10 Using HSS to Scan for Trojans

## Scenario

Trojans are an important issue in the current network security field. They intrude computer systems in different ways, which poses serious threats to user data security, privacy protection, and system stability.

To prevent Trojans, you need to update the OS and software in a timely manner, use secure network connections, and avoid downloading and running files from unknown sources. In addition, you can use HSS to view and handle reported Trojan alarms and fix system vulnerabilities to improve system security.

This section describes how to use HSS to scan for Trojans.

## Prerequisites

HSS professional, enterprise, premium, WTP, or container edition has been enabled for the server. For details, see **HSS Access Overview**.

## Step 1: Kill Trojans.

After you purchase and enable HSS for a server, if a Trojan is implanted on the server, HSS will send a Trojan alarm. You need to determine whether the detected Trojan alarm file is normal. If it is an attack event, you are advised to isolate and kill malicious files.

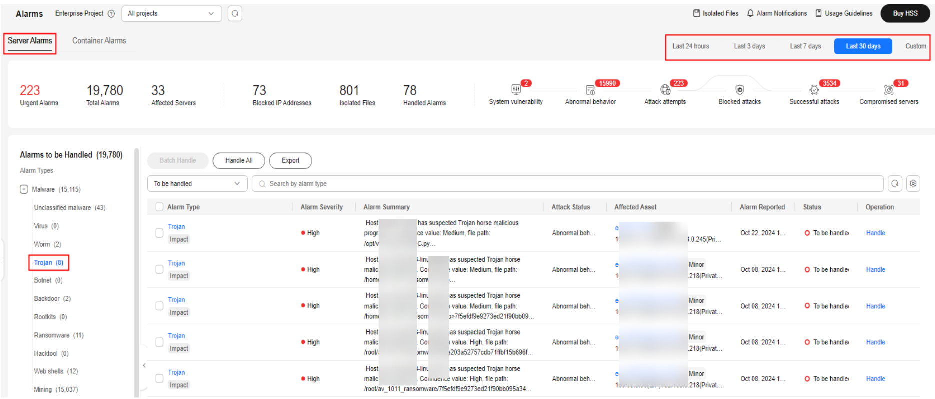
**Step 1** **Log in to the management console**.

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

**Step 3** In the navigation pane on the left, choose **Detection & Response > Alarms**. The **Server Alarms** page is displayed.

**Step 4** In the **Alarms to Be Handled** area, choose **Malware** > **Trojan** to view the alarms reported within the specified time range.

**Figure 10-1** Trojan alarm



| Alarm Type | Alarm Severity | Alarm Summary | Attack Status | Affected Asset | Alarm Reported | Status | Operation |
|---|---|---|---|---|---|---|---|
| Trojan<br>Impact | ● High | Host [redacted] has suspected Trojan horse malicious progr[redacted]ce value: Medium, file path: /opt/v[redacted]C.py… | Abnormal beh… | e[redacted]<br>1[redacted].0.245(Pri… | Oct 22, 2024 1… | ○ To be handle | Handle |
| Trojan<br>Impact | ● High | Host [redacted]-linu[redacted]as suspected Trojan horse malic[redacted]. Co[redacted]e value: Medium, file path: /hom[redacted]som[redacted]… | Abnormal beh… | e[redacted] Minor<br>1[redacted].218(Privat… | Oct 08, 2024 1… | ○ To be handle | Handle |
| Trojan<br>Impact | ● High | Host [redacted]-linu[redacted]as suspected Trojan horse malic[redacted]. Co[redacted]e value: Medium, file path: /hom[redacted]som[redacted]>7f5efdf9e9273ed21f90bb09… | Abnormal beh… | e[redacted] Minor<br>1[redacted].218(Privat… | Oct 08, 2024 1… | ○ To be handle | Handle |
| Trojan<br>Impact | ● High | Host [redacted]-linu[redacted]as suspected Trojan horse malic[redacted]. Co[redacted]e value: High, file path: /root/[redacted]omw[redacted]e203a52757cdb71ffbf15b696f… | Abnormal beh… | e[redacted] Minor<br>1[redacted].218(Privat… | Oct 08, 2024 1… | ○ To be handle | Handle |
| Trojan<br>Impact | ● High | Host [redacted]-linu[redacted]as suspected Trojan horse malic[redacted]. Confidence value: High, file path: /root/av_1011_ransomware/7f5efdf9e9273ed21f90bb095a34… | Abnormal beh… | e[redacted] Minor<br>1[redacted].218(Privat… | Oct 08, 2024 1… | ○ To be handle | Handle |

**Step 5** In the alarm list on the right, click the alarm name to view details about the Trojan alarm.

**Step 6** In the alarm list, click **Handle** in the **Operation** column.

**Step 7** In the dialog box that is displayed, set **Action** to **Isolate and kill**.

If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers.

**----End**

## Step 2: Data Backup and Restoration and Vulnerability Fixing

- Data backup and restoration

  If your data is lost due to Trojan malicious programs and you have subscribed to CBR, you can try to restore data using CBR. For details, see **Restoring Data Using a Cloud Server Backup**.

- Vulnerability fixing

  To prevent the server from being intruded by Trojans again, you can use the vulnerability management function of HSS to view and fix the server vulnerabilities. For details, see **Using HSS to Scan and Fix Vulnerabilities**.

# 11 Using HSS to Handle Mining Attacks

## Scenario

Mining, also called cryptocurrency mining, is a process of obtaining encrypted currencies through a large number of computing. The process occupies victims' system and network resources and obtaining digital currency. To reduce costs, mining programs are implanted into personal or enterprise computers and mobile devices without permissions.

Take immediate measures to contain the attack to your server, preventing miners from occupying CPU or affecting other applications. If a server is intruded by a mining program, the mining program may penetrate the intranet and persist on the intruded server. In addition, attackers may use mining programs to obtain confidential information, such as confidential files and the usernames and passwords of key assets.

HSS can detect and respond to mining attacks. It can detect and isolate mining virus software. This section describes how to harden your servers to better block intrusions using HSS.

## Prerequisites

HSS professional, enterprise, premium, WTP, or container edition has been enabled for the server. For details, see **HSS Access Overview**.

## During Attack: Quickly Block the Mining Program

1. **Handle the mining alarm and terminate the malicious process.**
   a. **Log in to the management console**.
   b. In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.
   c. In the navigation pane on the left, choose **Detection & Response > Alarms**. The **Server Alarms** page is displayed.

   NOTE

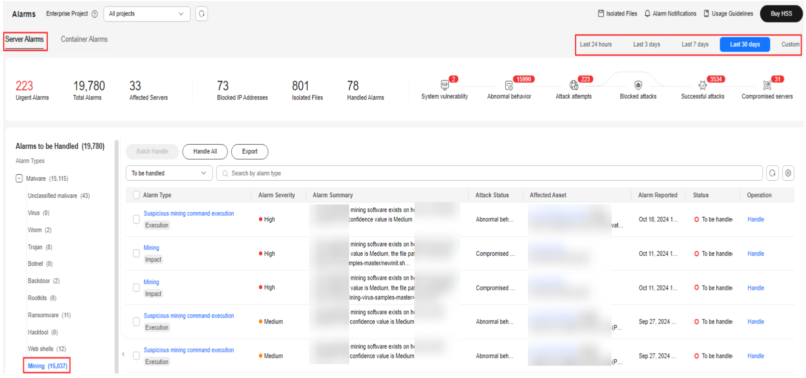
   If your servers are managed by enterprise projects, you can select the target enterprise project to view or operate the asset and detection information.

d. Check and handle **Mining** alarms.

When a mining program is implanted on a server, HSS sends a mining alarm. You need to determine whether the detected mining alarm file is normal. If it is an attack event, you are advised to isolate and kill mining program.

i. In the **Alarms to Be Handled** area, choose **Malware** > **Mining**.

**Figure 11-1** Mining alarm



| Alarm Type | Alarm Severity | Alarm Summary | Attack Status | Affected Asset | Alarm Reported | Status | Operation |
|---|---|---|---|---|---|---|---|
| Suspicious mining command execution<br>Execution | High | [redacted] mining software exists on h<br>confidence value is Medium | Abnormal beh... | [redacted] vat... | Oct 18, 2024 1... | To be handle | Handle |
| Mining<br>Impact | High | [redacted] mining software exists on h<br>value is Medium, the file pa<br>mples-master/newinit.sh... | Compromised ... | [redacted] | Oct 11, 2024 1... | To be handle | Handle |
| Mining<br>Impact | High | [redacted] mining software exists on h<br>value is Medium, the file pa<br>ining-virus-samples-master | Compromised ... | [redacted] | Oct 11, 2024 1... | To be handle | Handle |
| Suspicious mining command execution<br>Execution | Medium | [redacted] mining software exists on h<br>confidence value is Medium | Abnormal beh... | [redacted] (P... | Sep 27, 2024 ... | To be handle | Handle |
| Suspicious mining command execution<br>Execution | Medium | [redacted] mining software exists on h<br>confidence value is Medium | Abnormal beh... | [redacted] (P... | Sep 27, 2024 ... | To be handle | Handle |

ii. In the alarm list on the right, click the alarm name to view the alarm details.

iii. In the alarm list, click **Handle** in the **Operation** column.

iv. In the dialog box that is displayed, set **Action** to **Isolate and kill**.

If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers.

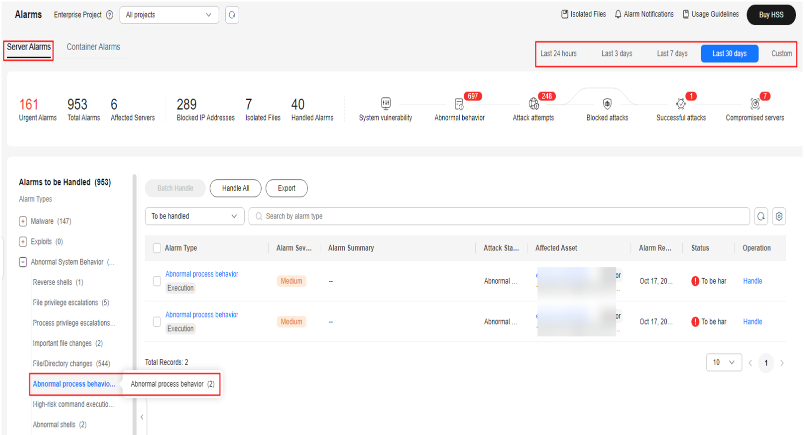
v. Click **OK**.

e. **View and handle the Abnormal Process Behavior alarm.**

Check **Abnormal process behavior** events. You need to determine whether the detected abnormal processes are proper. If it is confirmed that processes are unreasonable, you are advised to isolate and kill them.

i. In the **Alarms to Be Handled** area, choose **Abnormal System Behavior** > **Abnormal process behavior**.

**Figure 11-2** Abnormal process behavior



| Alarm Type | Alarm Sev... | Alarm Summary | Attack Sta... | Affected Asset | Alarm Re... | Status | Operation |
|---|---|---|---|---|---|---|---|
| Abnormal process behavior<br>Execution | Medium | -- | Abnormal ... | [redacted] | Oct 17, 20... | To be har | Handle |
| Abnormal process behavior<br>Execution | Medium | -- | Abnormal ... | [redacted] | Oct 17, 20... | To be har | Handle |

Total Records: 2

10 ‹ 1 ›

  ii. In the alarm list on the right, click the alarm name to view the alarm details.

  iii. In the alarm list, click **Handle** in the **Operation** column.

  iv. In the dialog box that is displayed, set **Action** to **Isolate and kill**.

  v. Click **OK**.

2. **Check auto-startup items to eliminate mining threats.**

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

   a. In the navigation tree on the left, choose **Asset Management > Server Fingerprints**. The **Server Fingerprints** page is displayed.

   b. Click **Auto-startup** and click the **Operation History** tab to view the historical changes.

3. **Scan the attacked server and scan for viruses.**

   HSS provides the virus scanning and removal function. The function uses the virus detection engine to scan virus files on the server. You can quickly scan attacked servers to eliminate potential malicious threats. You need to determine whether the scanned virus files are proper. If not, you are advised to isolate them.

   a. In the navigation tree on the left, choose **Server Protection > Virus Scan**. The **Virus Scan** page is displayed.

   b. Click **Quick Scan**.

   c. Set parameters related to the **Quick Scan** task as prompted.

      Select the server that is attacked by mining and retain the default values for other parameters. For more information, see **Quick Scan**.

   d. Click **Scan**.

   e. After the scanning task is complete, you can view the virus files in the lower part of the **Virus Scan** page.

   f. In the **Operation** column of a virus file, click **Handle**.

   g. In the dialog box that is displayed, set **Action** to **Manual isolation**.

      After a file is isolated, the read/write operation cannot be performed on the virus-infected file. Files that have been isolated are added to the **Isolated Files**. You can restore or delete them in the **Isolated Files**.

   h. Click **OK**.

## After Attack: Perform Security Hardening on the Server

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

- **Linux servers**

  a. Let HSS automatically scan your servers and applications in the early morning every day to help you detect and eliminate security risks.

  b. Set stronger passwords for all accounts (including system and application accounts), or change the login mode to key-based login.

     i. Set the security password. For details, see **How Do I Set a Secure Password?**.

ii. Use the key to log in to the server. For details, see **Using a Private Key to Log In to the Linux ECS**.

c. Strictly control the usage of system administrator accounts. Grant only the least permissions required for applications and middleware and strictly control their usage.

d. 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**

| Account | 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. |
| 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. |

| Account | Description | Procedure |
|---|---|---|
| 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 displayed dialog box, select **Enable** and click **OK**. |

– **Password hardening**

| Password | Description | Procedure |
|---|---|---|
| Complexity | In line with the requirements set 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. |
| 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. |
| 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). Access from other terminals are not allowed. | 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. |

# 12 Using HSS to Monitor the Integrity of Linux Server Files

## Scenario

File integrity means that the file content is not modified, deleted, or damaged without authorization during storage, transmission, and processing, ensuring the authenticity and reliability. Ensure file integrity in server security protection includes but is not limited to the following aspects:

- Data tampering prevention: File integrity monitoring prevents attackers from maliciously tampering with or damaging data and prevents data damage caused by software faults or misoperations of internal personnel, ensuring data integrity and authenticity.
- Improving server security: File integrity monitoring helps you quickly identify unauthorized file modification and take corresponding security measures, reducing potential security risks and improving server defense capabilities.
- Meet compliance requirements: Many industry standards and regulations require enterprises and organizations to protect the integrity and security of sensitive data. By monitoring file integrity, you can avoid legal risks and fines for data security issues.

HSS provides the server security alarm and file integrity management functions. HSS can monitor files or directories on the server and generate alarms for suspicious file or directory modification. This section describes how to use HSS functions to monitor the integrity of Linux server files.

## Differentiated File Protection in Server Security Alarm and File Integrity Management

Both the server security alarm function and file integrity management function of HSS provide file integrity monitoring capabilities. The two functions can provide comprehensive security protection for files. For details about the differences, see **Table 12-1**.

**Table 12-1** Differentiated file protection in server security alarms and file integrity management

| Type | Server Alarms | File Integrity Monitoring (FIM) |
|---|---|---|
| Monitoring type | Files and directories | File |
| Alarm type | ● File privilege escalation: An alarm is generated for file privilege escalation.<br>● File/Directory change: Monitors system files/ directories in real time, and generates alarms for operations such as creating, deleting, moving, modifying attributes, or modifying content. | Key file change: Monitors key system files (such as ls, ps, login, and top) in real time and generates alarms for file content modification operations. |
| File protection principle | Conduct analysis based on behavior characteristics and focus on suspicious behaviors or activities. | Focus on the integrity of the file and determine whether the current file status is different from the last time by comparing the file status. |
| Supported OS | ● File privilege escalation: Linux<br>● File/Directory changes: Windows and Linux | Linux |
| Advantages | You can monitor not only files, but also directories, and monitor more types for changing files. | File change records are stored permanently, helping O&M personnel investigate the behavior of attackers. |

## Prerequisites

HSS Professional, Enterprise, Premium, Web Tamper Protection, or Container Edition has been enabled for the server. For details, see **HSS Access Overview**.

## Procedure

**Step 1** **Configuration file protection policy.**

1. **Log in to the management console**.
2. In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.
3. In the navigation pane, choose **Security Operations** > **Policies**.

NOTE

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

4. Click the name of the policy group to access the policy detail list.

   HSS provides multiple preset policy groups. After protection is enabled for a server, the preset system group is bound by default. You can also click **Copy** in the **Operation** column of a policy group. For details, see **Creating a Custom Policy Group**.

5. Select the **File Protection** policy and click **Enable** in the **Operation** column to enable file protection detection.

   The file protection policy is enabled by default. If you have disabled the policy, you need to enable it.

6. Click the **File Protection** policy. The policy details page is displayed.

7. Customize the monitoring file directory and monitoring operation type. For details about the parameters, see **Table 12-2**.

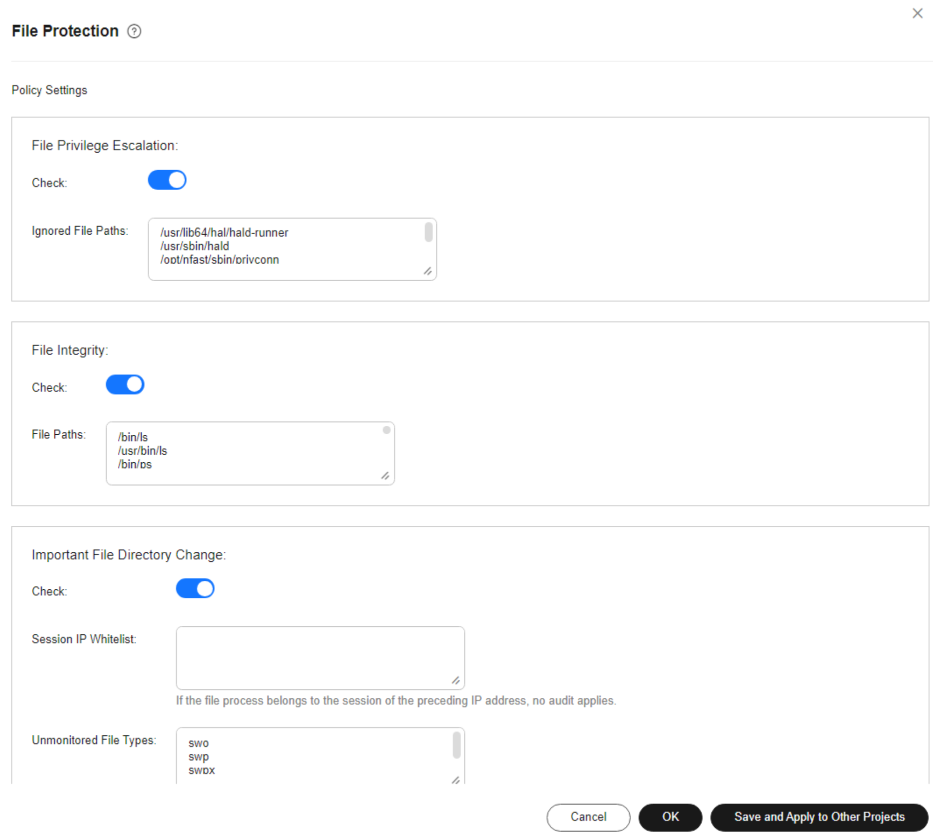
   **Table 12-2** displays the default values of file protection policies. You can customize file protection policies based on the site requirements. To prevent a large number of false alarms caused by file integrity changes and increase the O&M workload, you are advised to configure file protection policies as follows:

   a. Small-scale trial: When configuring the file protection policy for the first time, you are advised to perform the trial on a few servers.

   b. Policy tuning: Pay attention to the accuracy and applicability of policies during the validity period, and further improve the configured policies based on the results to reduce false positives.

   c. Formal application: After multiple policies tuning, if the matching result becomes stable and the false positives almost do not exist, the policy can be applied to more servers.

**Figure 12-1** File protection policy



File Protection ⓘ

Policy Settings

File Privilege Escalation:

Check: ●

Ignored File Paths:

```
/usr/lib64/hal/hald-runner
/usr/sbin/hald
/opt/nfast/sbin/privconn
```

File Integrity:

Check: ●

File Paths:

```
/bin/ls
/usr/bin/ls
/bin/ps
```

Important File Directory Change:

Check: ●

Session IP Whitelist:

If the file process belongs to the session of the preceding IP address, no audit applies.

Unmonitored File Types:

```
swo
swp
swpx
```

**Table 12-2** Parameter description

| Policy Module | Parameter | Default Parameter Value | Description |
|---|---|---|---|
| File Privilege Escalation | Check | **Enabled** | Detects privilege escalation.<br>– ●: enabled<br>– ○: disabled |
| | Ignored File Paths | – **/usr/lib64/hal/hald-runner**<br>– **/usr/sbin/hald**<br>– **/opt/nfast/sbin/privconn**<br>– **/usr/sbin/dhclient**<br>– **/usr/sbin/tcpdump** | Enter the path of the file to be ignored.<br>Start the path with a slash (/) and do not end it with a slash (/). Each path occupies a line. No spaces are allowed between path names. |

| Policy Module | Parameter | Default Parameter Value | Description |
|---|---|---|---|
| File Integrity | Check | **Enabled** | Detects the integrity of key files.<br>– ●: enabled<br>– ○: disabled |
| | File Paths | – **/bin/ls**<br>– **/usr/bin/ls**<br>– **/bin/ps**<br>– **/usr/bin/ps**<br>– **/bin/bash**<br>– **/usr/bin/bash**<br>– **/bin/login**<br>– **/usr/bin/login**<br>– **/usr/bin/passwd**<br>– **/usr/bin/top**<br>– **/usr/bin/killall**<br>– **/usr/bin/ssh**<br>– **/usr/bin/wget**<br>– **/usr/bin/curl** | Enter the path of the file.<br>Start the path with a slash (/) and do not end it with a slash (/). Each path occupies a line. No spaces are allowed between path names. |
| Important File Directory Change | Check | **Enabled** | Detects the directory change of key files.<br>– ●: enabled<br>– ○: disabled |
| | Session IP Whitelist | - | If the file process belongs to the sessions of the whitelisted IP addresses, the process is not audited. |
| | Unmonitored File Types | – **swo**<br>– **swp**<br>– **swpx**<br>– **lck** | Suffix of the file type that is ignored. |

| Policy Module | Parameter | Default Parameter Value | Description |
|---|---|---|---|
| | Unmonitored File Paths | – **/etc/init.d/.depend.start**<br>– **/etc/init.d/.depend.stop**<br>– **/etc/init.d/.depend.halt**<br>– **/etc/init.d/.depend.boot**<br>– **/var/spool/cron/sed*** | Enter the path of the file to be ignored. |
| | Monitoring Login Keys | **Enable and select Monitor Creation, Monitor Deletion, Monitor Movement, and Monitor Modification.** | Whether to enable the monitoring of login keys.<br>– ●: enabled<br>– ○: disabled |

| Policy Module | Parameter | Default Parameter Value | Description |
|---|---|---|---|
| | Directory Monitoring Mode | **There are many file directories to be monitored. The following describes only some monitoring paths. For details, go to the HSS management console.**<br>– **/etc/rc.d/rc.local**<br>– **/etc/cron.allow**<br>– **/etc/crontab**<br>– **/var/spool/cron/root**<br>– **/var/spool/cron/root**<br>– **/etc/cron.allow**<br>– **/etc/passwd**<br>– **/etc/profile.d/zzz_euleros_history.sh**<br>– **/etc/profile** | The value of directory monitoring modes can be **Conservative** or **Sensitive**. Compared with the **Conservative** mode, the **Sensitive** mode monitors more file or directory paths by default.<br>In the two modes, some file or directory monitoring paths are preset. You can add or delete them as required.<br>– **File or Directory Path**: path of the file or directory to be monitored. Up to 50 paths can be added. Ensure the specified paths are valid.<br>– **Alias**: alias of a file or directory path. You can enter a name that is easy to distinguish.<br>– **Monitor Subdirectory**: If this option is selected, all files in the corresponding subdirectories are monitored. If it is not selected, subdirectories are not monitored.<br>– **Monitor Creation**, **Monitor Deletion**, **Monitor Movement**, and **Monitor Modification**: Select them as needed. |

**Step 2** **(Optional) Deploy a policy for the server.**

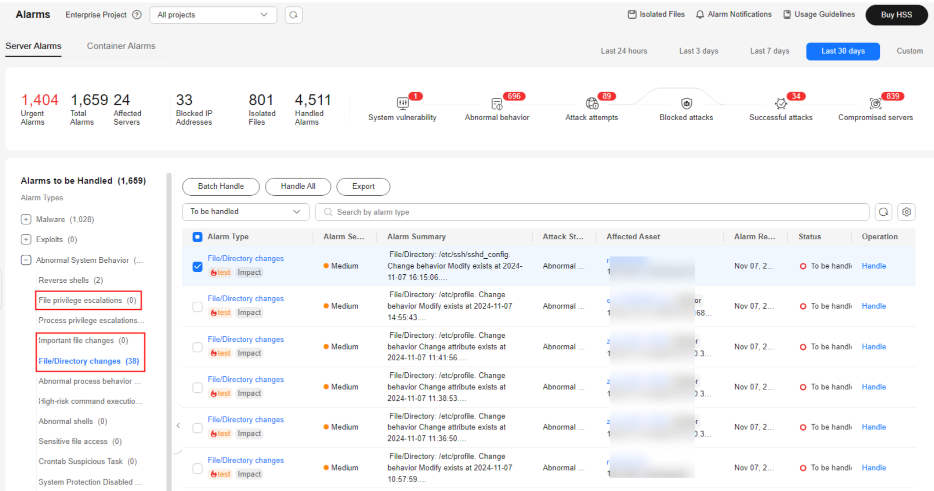
If you configure a file protection policy based on a newly created custom policy group in **Step 1**, you need to deploy the new policy group and apply it to the target server after creating and configuring the policy group. For details, see **Deploying a Protection Policy**.

**Step 3** **View and handle file change alarms.**

HSS monitors the files or directory paths configured in the file protection policy in real time and generates alarms once detecting abnormal changes. After receiving an alarm, handle the alarm in a timely manner.

1. In the navigation pane on the left, choose **Detection & Response** > **Alarms**. The **Server Alarms** page is displayed.
2. In the list of alarms to be handled, expand **Abnormal System Behavior** and focus on several types of alarms related to file changes, as shown in Figure 12-2.

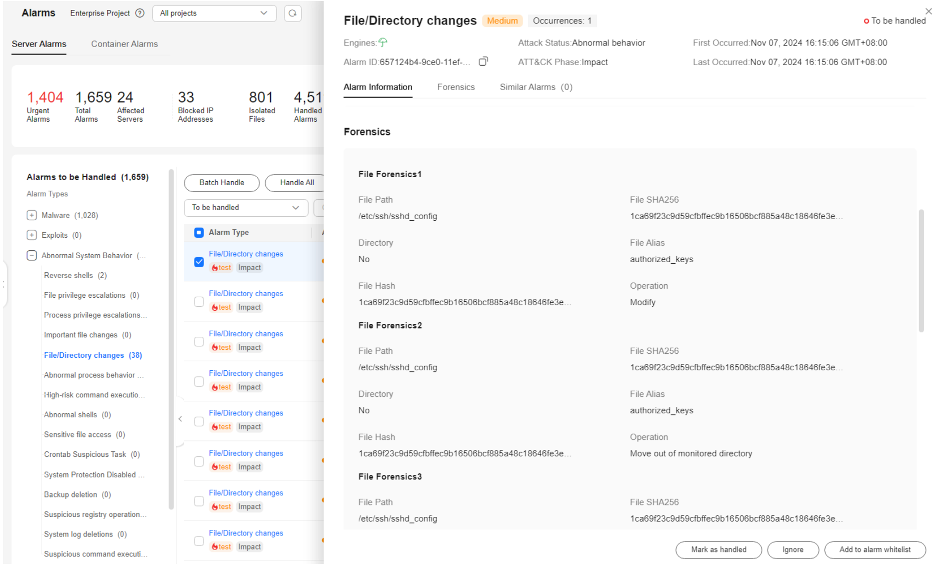
**Figure 12-2** Alarms related to file changes



| Alarm Type | Alarm Se... | Alarm Summary | Attack St... | Affected Asset | Alarm Re... | Status | Operation |
|---|---|---|---|---|---|---|---|
| ☑ File/Directory changes test Impact | Medium | File/Directory: /etc/ssh/sshd_config. Change behavior Modify exists at 2024-11-07 16:15:06.... | Abnormal ... | [redacted] | Nov 07, 2... | To be handl | Handle |
| □ File/Directory changes test Impact | Medium | File/Directory: /etc/profile. Change behavior Modify exists at 2024-11-07 14:55:43.... | Abnormal ... | [redacted] | Nov 07, 2... | To be handl | Handle |
| □ File/Directory changes test Impact | Medium | File/Directory: /etc/profile. Change behavior Change attribute exists at 2024-11-07 11:41:56.... | Abnormal ... | [redacted] | Nov 07, 2... | To be handl | Handle |
| □ File/Directory changes test Impact | Medium | File/Directory: /etc/profile. Change behavior Change attribute exists at 2024-11-07 11:38:53.... | Abnormal ... | [redacted] | Nov 07, 2... | To be handl | Handle |
| □ File/Directory changes test Impact | Medium | File/Directory: /etc/profile. Change behavior Change attribute exists at 2024-11-07 11:36:50.... | Abnormal ... | [redacted] | Nov 07, 2... | To be handl | Handle |
| □ File/Directory changes test Impact | Medium | File/Directory: /etc/profile. Change behavior Modify exists at 2024-11-07 10:57:59.... | Abnormal ... | [redacted] | Nov 07, 2... | To be handl | Handle |

3. Click an alarm of any type. In the alarm list on the right, click the alarm name to view the details.

**Figure 12-3** Viewing alarm details



File/Directory changes Medium Occurrences: 1 ○ To be handled

Engines:
Attack Status:Abnormal behavior
First Occurred:Nov 07, 2024 16:15:06 GMT+08:00
Alarm ID:657124b4-9ce0-11ef-...
ATT&CK Phase:Impact
Last Occurred:Nov 07, 2024 16:15:06 GMT+08:00

Forensics

File Forensics1

| | |
|---|---|
| File Path<br>/etc/ssh/sshd_config | File SHA256<br>1ca69f23c9d59cfbffec9b16506bcf885a48c18646fe3e... |
| Directory<br>No | File Alias<br>authorized_keys |
| File Hash<br>1ca69f23c9d59cfbffec9b16506bcf885a48c18646fe3e... | Operation<br>Modify |

File Forensics2

| | |
|---|---|
| File Path<br>/etc/ssh/sshd_config | File SHA256<br>1ca69f23c9d59cfbffec9b16506bcf885a48c18646fe3e... |
| Directory<br>No | File Alias<br>authorized_keys |
| File Hash<br>1ca69f23c9d59cfbffec9b16506bcf885a48c18646fe3e... | Operation<br>Move out of monitored directory |

File Forensics3

| | |
|---|---|
| File Path<br>/etc/ssh/sshd_config | File SHA256<br>1ca69f23c9d59cfbffec9b16506bcf885a48c18646fe3e... |

4. Handle the alarm based on the **Forensics** information in the alarm details.
   - **Alarms caused by normal operations.**

     In the lower right corner of the alarm details page, click **Ignore** to ignore the alarm.

- **Alarms caused by malicious files or programs.**
  1. Check whether high-risk alarms, such as reverse shell, abnormal login, and malware, are generated on the server. If yes, the server may be attacked. Perform a security check on the server immediately.
  2. In the lower right corner of the alarm details page, click **Mark as handled** to clear the alarm.

**Step 4 View the file change history.**

The file integrity management page keeps file change records on the server, helping you locate suspicious changes.

1. In the navigation pane on the left, choose **Server Protection > File Integrity Monitoring**. The **File Integrity Monitoring** page is displayed.
2. View the file changes on the ECS.

**----End**

# 13 Whitelist Can Be Used to Avoid False Alarm Reporting

## Scenario

HSS provides intrusion detection for servers and containers. It can detect various malicious behaviors or attacks, such as brute-force attacks, abnormal processes, web shells, and malware, and report alarms to users in a timely manner. Alarms received by users may include alarms triggered by normal services. In this case, users can whitelist the alarms so that alarms are ignored by trusted objects, reducing O&M workload and improving O&M efficiency.

This section describes how to use the whitelist to prevent false alarms.

## Whitelist Mechanism

HSS provides two whitelist mechanisms to handle alarms, which are alarm whitelist and detection policy whitelist. HSS does not generate alarms for whitelisted objects. For details about the two types of whitelists, see **Table 13-1**.

**Table 13-1** Whitelist mechanism

| Whitelist Mechanism | Description | Advantage | Disadvantage |
|---|---|---|---|
| Alarm whitelist | When handling alarms, you can add alarms to the whitelist and configure whitelist rules. HSS only detects but does not report alarms for abnormal events that match the whitelist rules. | HSS automatically associates preset whitelist rules based on the alarm content. You can quickly whitelist alarms when handling them. | The whitelist cannot be added in advance. You can only wait until the alarm is triggered. |

| Whitelist Mechanism | Description | Advantage | Disadvantage |
|---|---|---|---|
| Detection policy whitelist | HSS detects servers using agent. The detection scope of the agent can be controlled by the policy delivered on the console. Therefore, you can whitelist trusted objects in the policy. After the policy is delivered, HSS does not generate alarms for whitelisted objects. | ● You can add trusted objects to the whitelist in advance without waiting for alarms to be triggered.<br>● Alarm whitelists cannot be added for container alarms, such as pods, images, and organizations. You can add detection policy whitelists. | Alarms that have been generated cannot be processed synchronously. |

## Add to Alarm Whitelist

The process of adding an alarm whitelist for server security alarms and container security alarms is similar. The following uses the high-risk command execution alarm as an example.

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

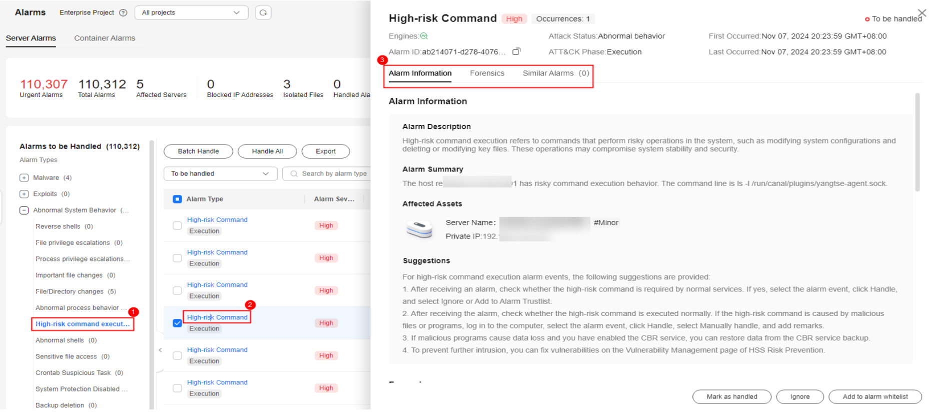
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

**Step 3** In the navigation tree on the left, choose **Detection & Response** > **Alarms**. On the **Server Alarms** tab page, view the reported alarms.

**Step 4** Click the alarm name to view the details and check whether the alarm is triggered by a normal service.

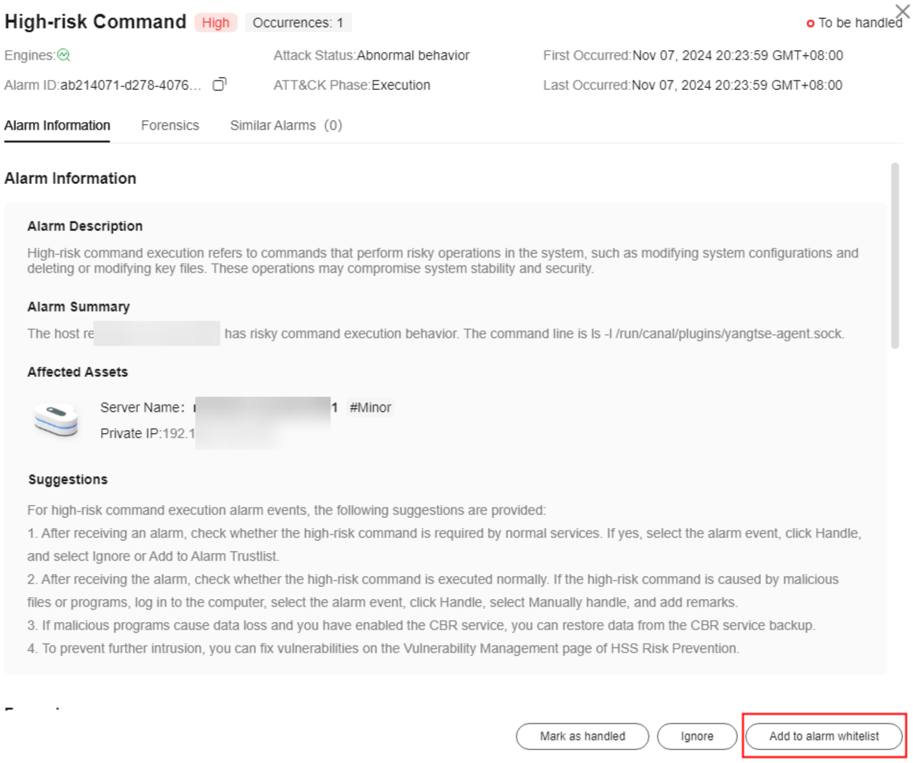
View **Alarm Information**, **Forensics**, and **Similar Alarms** in the alarm details to check whether the command execution is triggered by normal services.

**Figure 13-1** Viewing alarm details



**Step 5** If the alarm is triggered by normal services, click **Add to alarm whitelist**.

**Figure 13-2** Adding to alarm whitelist



Engines:

Attack Status:Abnormal behavior

First Occurred:Nov 07, 2024 20:23:59 GMT+08:00

Alarm ID:ab214071-d278-4076...

ATT&CK Phase:Execution

Last Occurred:Nov 07, 2024 20:23:59 GMT+08:00

Alarm Information

Alarm Description

High-risk command execution refers to commands that perform risky operations in the system, such as modifying system configurations and deleting or modifying key files. These operations may compromise system stability and security.

Alarm Summary

The host re has risky command execution behavior. The command line is ls -l /run/canal/plugins/yangtse-agent.sock.

Affected Assets

Server Name: l 1 #Minor

Private IP:192.1

Suggestions

For high-risk command execution alarm events, the following suggestions are provided:

1. After receiving an alarm, check whether the high-risk command is required by normal services. If yes, select the alarm event, click Handle, and select Ignore or Add to Alarm Trustlist.

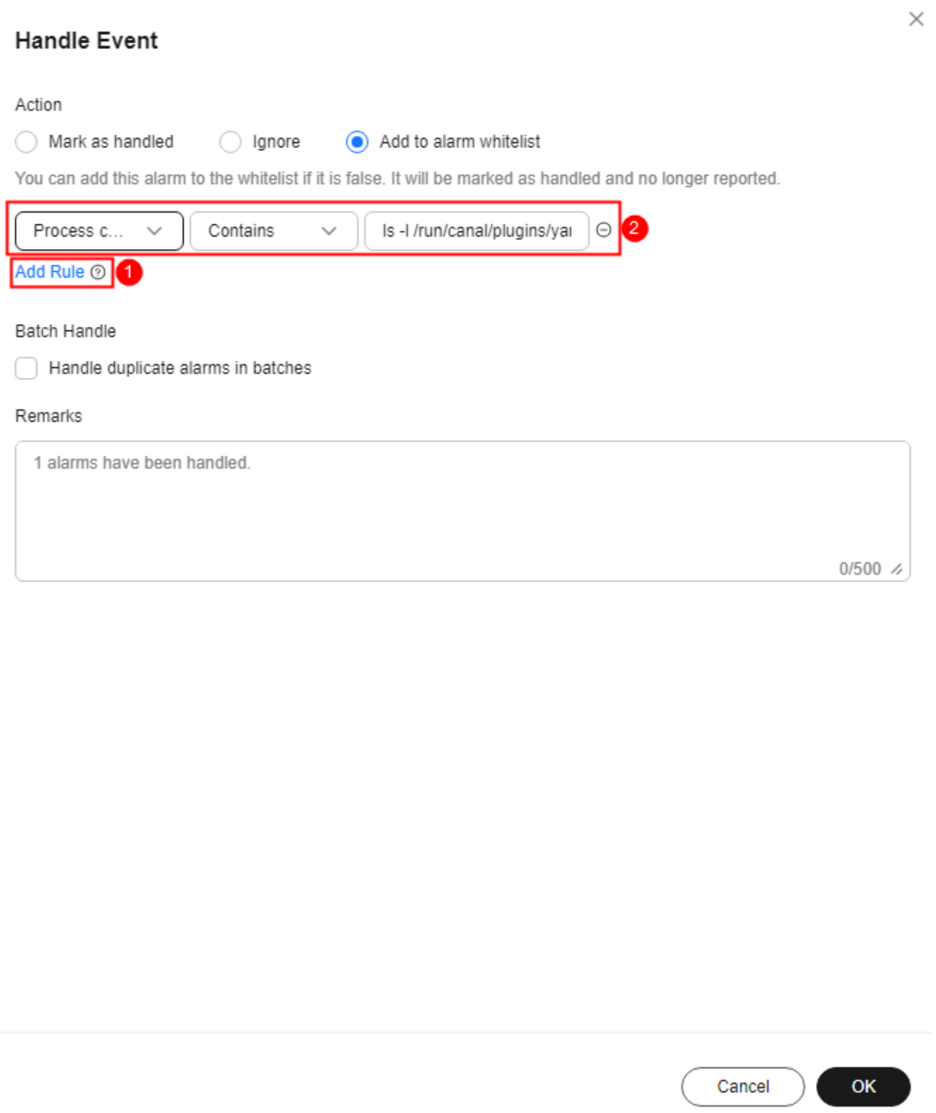
2. After receiving the alarm, check whether the high-risk command is executed normally. If the high-risk command is caused by malicious files or programs, log in to the computer, select the alarm event, click Handle, select Manually handle, and add remarks.

3. If malicious programs cause data loss and you have enabled the CBR service, you can restore data from the CBR service backup.

4. To prevent further intrusion, you can fix vulnerabilities on the Vulnerability Management page of HSS Risk Prevention.

**Step 6** In the **Handle Event** area, click **Add Rule** and configure an alarm whitelist trigger rule. Table 13-2 describes the parameters.

**Figure 13-3** Alarm whitelist rules



Handle Event

Action

○ Mark as handled ○ Ignore ● Add to alarm whitelist

You can add this alarm to the whitelist if it is false. It will be marked as handled and no longer reported.

Process c... | Contains | ls -l /run/canal/plugins/yaı

Add Rule

Batch Handle

□ Handle duplicate alarms in batches

Remarks

1 alarms have been handled.

0/500

**Table 13-2** Alarm whitelist rules parameters

| Parameter | Example Value | Description |
|---|---|---|
| Whitelist Field | **Process command line** | The object types to be whitelisted. The following fields can be whitelisted for server security alarms:<br>● Process path<br>● Process command line<br>● File path<br>● User name<br>● Remote IP address<br>The fields that can be whitelisted vary according to the alarm type. |

| Parameter | Example Value | Description |
|---|---|---|
| Wildcard | **Include** | The following wildcards are supported:<br>● Include: HSS does not generate any alarm if the alarm information contains **Description** of the whitelist rule.<br>● If they are the same, HSS does not generate an alarm when the alarm information completely matches the **Description** of the whitelist rule. |
| Description | **ls -l /run/canal/plugins/yangtse-agent.sock** | HSS automatically adds the detected suspicious processes and files to the whitelist. The content can also be customized. |

NOTE

Multiple whitelist rules can be added for the same alarm. If multiple rules are added, the relationship between them is OR.

**Step 7** In the **Handle Event** area, click **OK**.

**----End**

## Adding a Detection Policy Whitelist

For details about the whitelist detection policies and alarms supported by HSS, see **Table 13-3**.

**Table 13-3** Adding a whitelist detection policy

| Policy Name | Alarm |
|---|---|
| Container information collection | Container mounting exception |
| Cluster intrusion detection | Kubernetes event deletion, privileged pods creation, interactive shells used in pod, pods created with sensitive directory, pod created with server network, pods created with host PID space, common pods access, APIServer authentication failure, API server access from common pod using cURL, Exec in system management space, pods created in system management space, static pod creations, DaemonSet creation, cluster scheduled tasks creation, List Secrets operations, allowed operation enumeration, high privilege RoleBinding or ClusterRoleBinding, and ServiceAccount creations |

| Policy Name | Alarm |
|---|---|
| Container escape | High-risk system calls, Shocker attacks, DirtCow attacks, and container file escape attacks |
| Container information module | Container namespace, container open port, container security options, and container mount directory |
| Container process whitelist | Abnormal container process |
| Fileless attack detection | Process injection, dynamic library injection, and memory file process |
| File protection | File directory change, key file change, and file privilege escalation |

| Policy Name | Alarm |
|---|---|
| HIPS detection | Windows Defender disabled, suspicious hacker tools, suspicious ransomware encryption behavior, hidden account creation, user password and credential reading, suspicious SAM file export, suspicious shadow copy deletion, backup file deletion, suspicious ransomware operation registry, suspicious abnormal process behavior, suspicious scanning and detection, suspicious ransomware script execution, suspicious mining command execution, suspicious windows security center disabling, suspicious behavior of disabling the firewall service, suspicious system automatic recovery disabling, executable file execution in Office, abnormal file creation with macros in Office, suspicious registry operation, Confluence remote code execution, MSDT remote code execution, Windows log clearing using Wevtutil, log removal using Fsutil, suspicious HTTP requests initiated by regsvr32, and load download using Windows Defender Windows remote command execution, Log4shell vulnerability execution, suspicious scheduled task operation, suspicious Windows command execution, Windows intrusion tool transmission, suspicious reverse shell command, remote suspicious script execution, suspicious software installation, perl reverse shell, awk reverse shell, python reverse shell, lua reverse shell, mkfifo/openssl reverse shell, php reverse shell, ruby reverse shell, reverse proxy using rssocks, bash reverse shell, ncat reverse shell, exec redirect reverse shell, node reverse shell, telnet dual port reverse shell, nc reverse shell, socat reverse shell, php_socket reverse shell, socket/tchsh reverse shell, modify files using vigr/vipw, system security logs clearing and replacement, SSH backdoors flexible connection, SSH keys replacement, install backdoors using curl/wget<br>Using proxy software tools, Python/Base64 execution, sudo privilege escalation vulnerability exploitation, adding system accounts whose UID is 0 (root permission), bypass command execution to modify permissions using $IFS, files or directories deletion using wipe, github sensitive information disclosure, ARP spoofing using commands, system database passwd records check, CVE/CNVD vulnerabilities downloaded by curl/wget/gcc, suspicious driver loading, uninstalling or stopping server installation program, obtain SSH credentials using strace, Golang reverse shell, detect intra-domain information using ldapsearch, detect privilege escalation vulnerabilities using perl script, detect privilege escalation vulnerabilities using bash script, detect privilege escalation vulnerabilities using python script, Enumy privilege escalation enumeration tool, Hydra brute-force attack tool, CDK container penetration tool, stowaway proxy tool, CF cloud penetration tool, Redis intrusion through redis-rogue-server, browser data collection through hack-browser-data, suspicious server detection behavior, suspicious download |

| Policy Name | Alarm |
|---|---|
| | behavior, suspicious interactive bash shell generation, sudo privilege escalation, vim privilege escalation, awk privilege escalation, obfuscated shell commands, hijacking of LD_PRELOAD dynamic link libraries, hijacking of dynamic linkers, suspicious sensitive file reading, suspicious sensitive file modification, socat port forwarding, ngrok port forwarding rinetd port forwarding, portmap port forwarding, portforward port forwarding, rakshasa port forwarding, hacker tool earthworm detection, suid/sgid privilege escalation, abnormal process behavior, suspicious scheduled task/auto-startup item creation, find privilege escalation, malicious domain names and malicious IP address access, reverse proxy using rcsocks/ssocks, SSH port forwarding, HashDump attacks, and procdump attacks |
| Login security check | Attempting brute-force attacks, brute force cracking success, user login success, remote login, user login rejection, first user login, and weak password of the system account |
| Malicious file detection | Abnormal shell, reverse shell, and malware |
| Port scan detection | Port scan |
| Root privilege escalation | Abnormal process behavior, suspicious process privilege escalation, and abnormal process external connection |
| Real-time process | High-risk command executions |
| Rootkit detection | Suspicious rootkit |

The detailed operations for configuring the whitelist in the preceding table are as follows:

NOTICE

If you configure a file protection policy based on a newly created custom policy group, you need to deploy the new policy group and apply it to the target server after creating and configuring the policy group. For details, see **Deploying a Protection Policy**.

## Container Information Collection

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

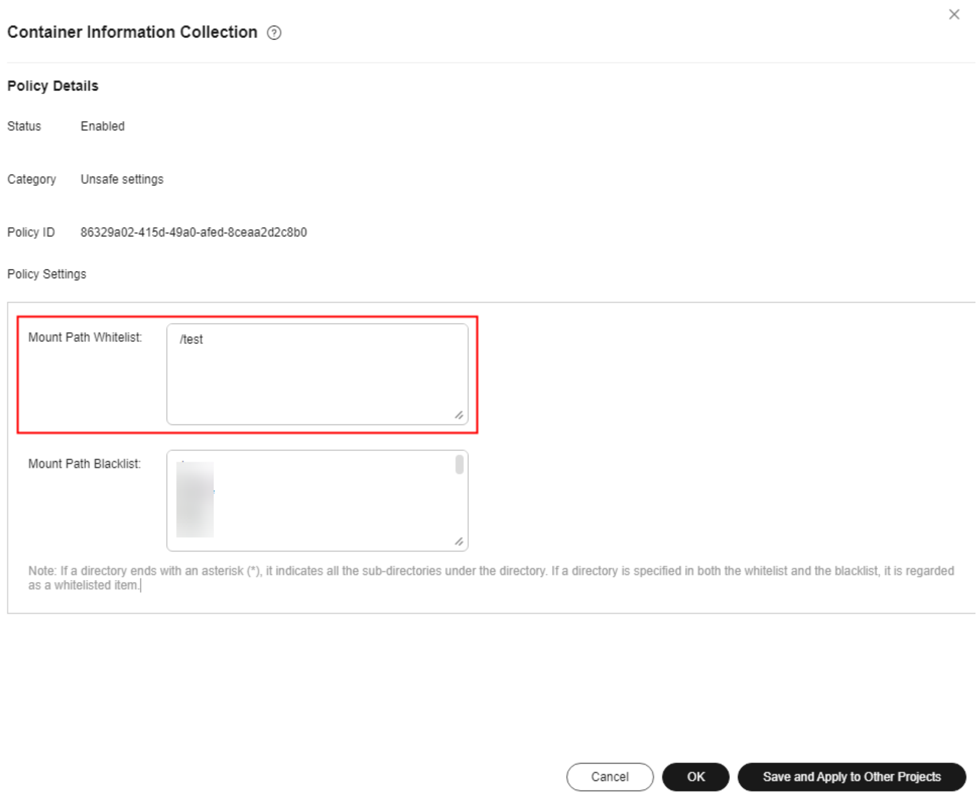
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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

**Step 4** Select the container policy group corresponding to the server and click the policy group name. The policy group details page is displayed.

**Step 5** Click the name of the **Container Information Collection** policy. On the policy details page, configure **Mount Path Whitelist**.

**Figure 13-4** Container information collection policy



Container Information Collection

Policy Details

Status Enabled

Category Unsafe settings

Policy ID 86329a02-415d-49a0-afed-8ceaa2d2c8b0

Policy Settings

Mount Path Whitelist: /test

Mount Path Blacklist:

Note: If a directory ends with an asterisk (*), it indicates all the sub-directories under the directory. If a directory is specified in both the whitelist and the blacklist, it is regarded as a whitelisted item.

**Table 13-4** Container information collection policy whitelist parameters

| Parameter | Examples | Description |
|---|---|---|
| Mount Path Whitelist | **/test** | Enter the mount directories that can be mounted. Use line breaks to separate multiple mount directory paths.<br>If a directory ends with an asterisk (*), it indicates all the sub-directories under the directory (excluding the main directory).<br>For example, if **/var/test/*** is specified in the whitelist, all sub-directories in **/var/test/** are whitelisted, excluding the **test** directory. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Cluster Intrusion Detection

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

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

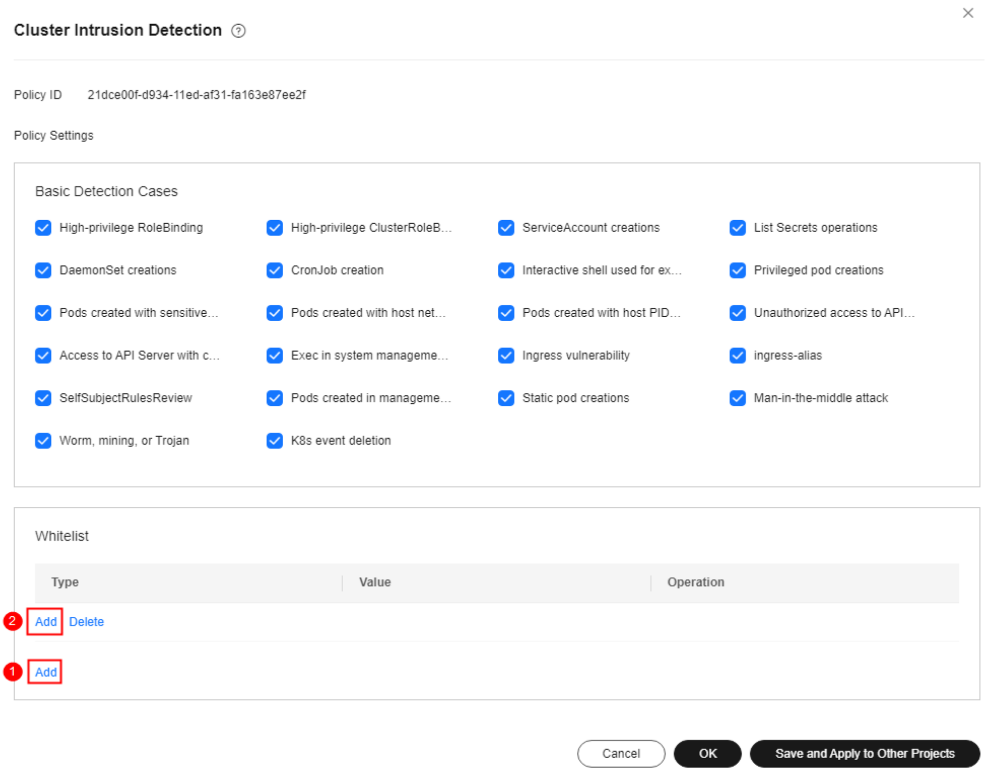
**Step 3** In the navigation pane, choose **Security Operations** > **Policies**.

**Step 4** Select the container policy group corresponding to the server and click the policy group name. The policy group details page is displayed.

**Step 5** Click the name of the target policy **Cluster Intrusion Detection**.

**Step 6** In the Whitelist area, click **Add** and then click **Add** to add a whitelist text box.

**Figure 13-5** Adding a whitelist entry



Cluster Intrusion Detection

Policy ID 21dce00f-d934-11ed-af31-fa163e87ee2f

Policy Settings

Basic Detection Cases

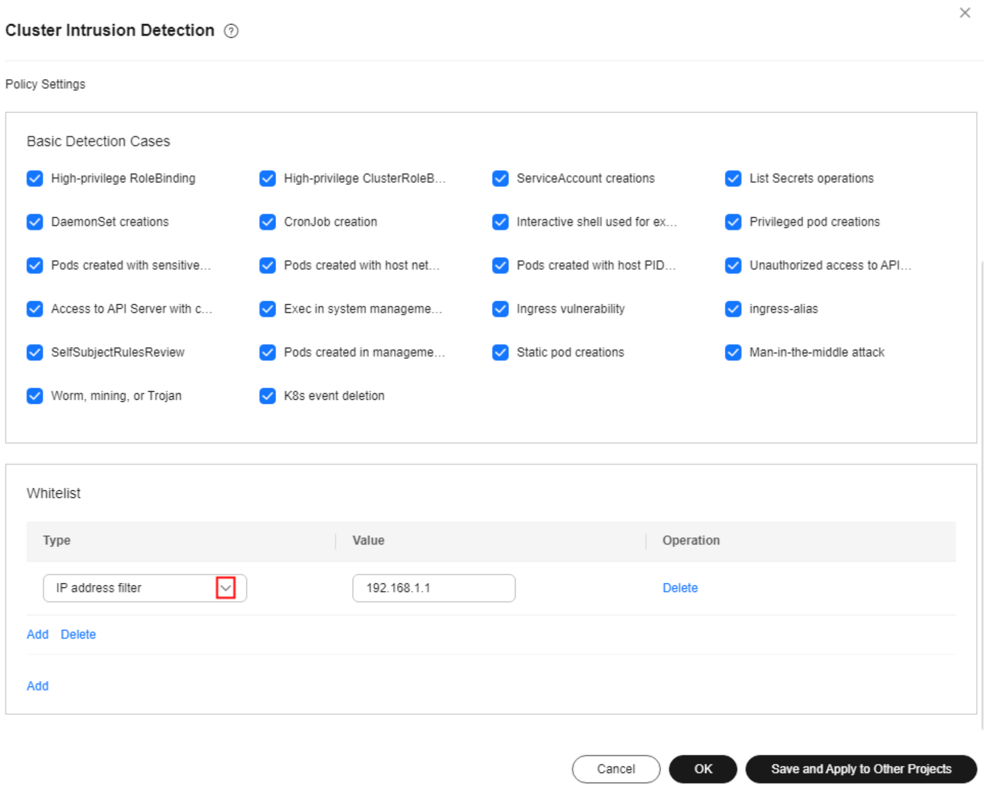
| | | | |
|---|---|---|---|
| ☑ High-privilege RoleBinding | ☑ High-privilege ClusterRoleB... | ☑ ServiceAccount creations | ☑ List Secrets operations |
| ☑ DaemonSet creations | ☑ CronJob creation | ☑ Interactive shell used for ex... | ☑ Privileged pod creations |
| ☑ Pods created with sensitive... | ☑ Pods created with host net... | ☑ Pods created with host PID... | ☑ Unauthorized access to API... |
| ☑ Access to API Server with c... | ☑ Exec in system manageme... | ☑ Ingress vulnerability | ☑ ingress-alias |
| ☑ SelfSubjectRulesReview | ☑ Pods created in manageme... | ☑ Static pod creations | ☑ Man-in-the-middle attack |
| ☑ Worm, mining, or Trojan | ☑ K8s event deletion | | |

Whitelist

| Type | Value | Operation |
|---|---|---|

**Step 7** Select a whitelist type from the **Type** drop-down list and enter a value.

**Figure 13-6** Cluster intrusion detection policy



Cluster Intrusion Detection ⓘ ×

Policy Settings

Basic Detection Cases

☑ High-privilege RoleBinding ☑ High-privilege ClusterRoleB... ☑ ServiceAccount creations ☑ List Secrets operations

☑ DaemonSet creations ☑ CronJob creation ☑ Interactive shell used for ex... ☑ Privileged pod creations

☑ Pods created with sensitive... ☑ Pods created with host net... ☑ Pods created with host PID... ☑ Unauthorized access to API...

☑ Access to API Server with c... ☑ Exec in system manageme... ☑ Ingress vulnerability ☑ ingress-alias

☑ SelfSubjectRulesReview ☑ Pods created in manageme... ☑ Static pod creations ☑ Man-in-the-middle attack

☑ Worm, mining, or Trojan ☑ K8s event deletion

Whitelist

| Type | Value | Operation |
|---|---|---|
| IP address filter | 192.168.1.1 | Delete |

Add Delete

Add

**Table 13-5** Cluster intrusion detection whitelist parameters

| Parameter | Example Value | Description |
|---|---|---|
| Type | **IP address filtering** | Customize the types to be ignored during detection.<br>The following types are supported:<br>● IP address filter<br>● Pod name filter<br>● Image name filter<br>● User filter<br>● Pod tag filter<br>● Namespace filter |
| Value | **192.168.1.1** | Enter the value of the type. In this example, select **IP address filter**. In this case, enter a specific IP address. |

**Step 8** Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Container Escape Policy

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

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

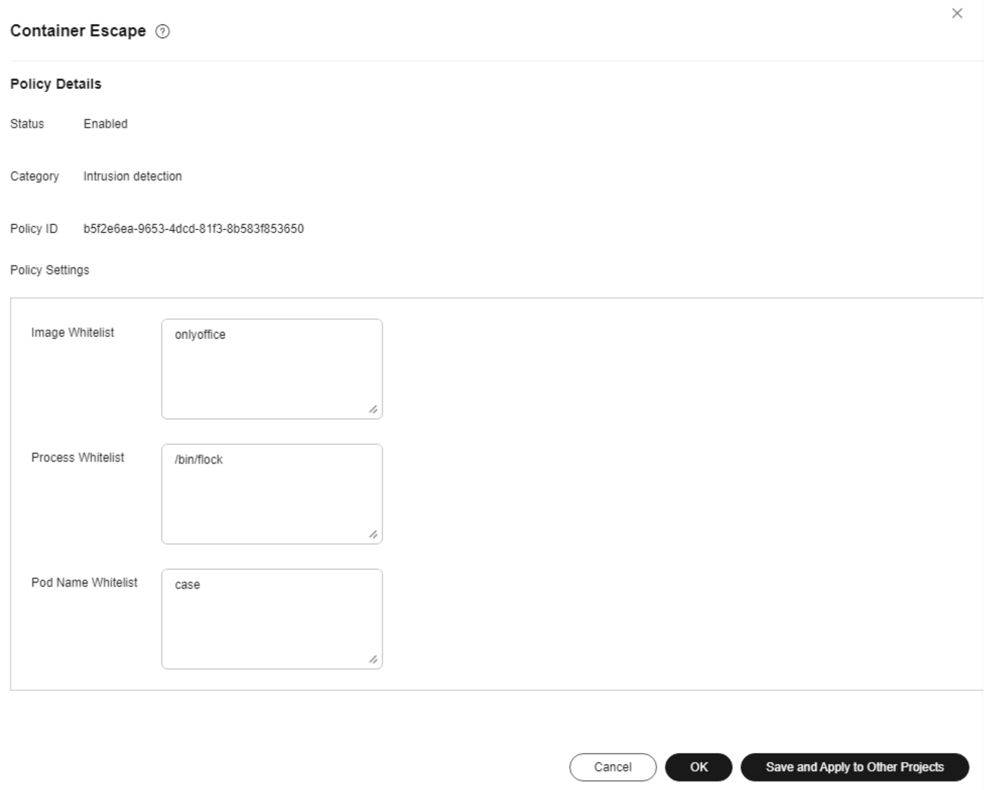
**Step 3** In the navigation pane, choose **Security Operations** > **Policies**.

**Step 4** Select the container policy group corresponding to the server and click the policy group name. The policy group details page is displayed.

**Step 5** Click the name of a **Container Escape** policy. On the policy details page that is displayed, configure the whitelist.

You can configure whitelists of different levels, such as images, processes, and pods. You can configure any type of whitelist as required.

**Figure 13-7** Container escape policy



Container Escape

Policy Details

Status Enabled

Category Intrusion detection

Policy ID b5f2e6ea-9653-4dcd-81f3-8b583f853650

Policy Settings

Image Whitelist: onlyoffice

Process Whitelist: /bin/flock

Pod Name Whitelist: case

**Table 13-6** Container escape detection policy whitelist parameters

| Parameter | Example Value | Description |
|---|---|---|
| Image Whitelist | **onlyoffice** | Enter the names of the images that do not need to perform container escape behavior detection. An image name can contain only letters, numbers, underscores (_), and hyphens (-), and each name needs to be on a separate line. Up to 100 image names are allowed. |
| Process Whitelist | **/bin/flock** | Enter the full paths of processes that do not need to perform container escape behavior detection. A process path can contain only letters, numbers, underscores (_), and hyphens (-), and each path needs to be on a separate line. Up to 100 process paths are allowed. |
| POD Name Whitelist | **case** | Enter the names of pods (not pod UIDs) that do not need to perform container escape behavior detection. A pod name can contain only letters, numbers, underscores (_), and hyphens (-), and each name needs to be on a separate line. Up to 100 pod names are allowed. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Container Information Module

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

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

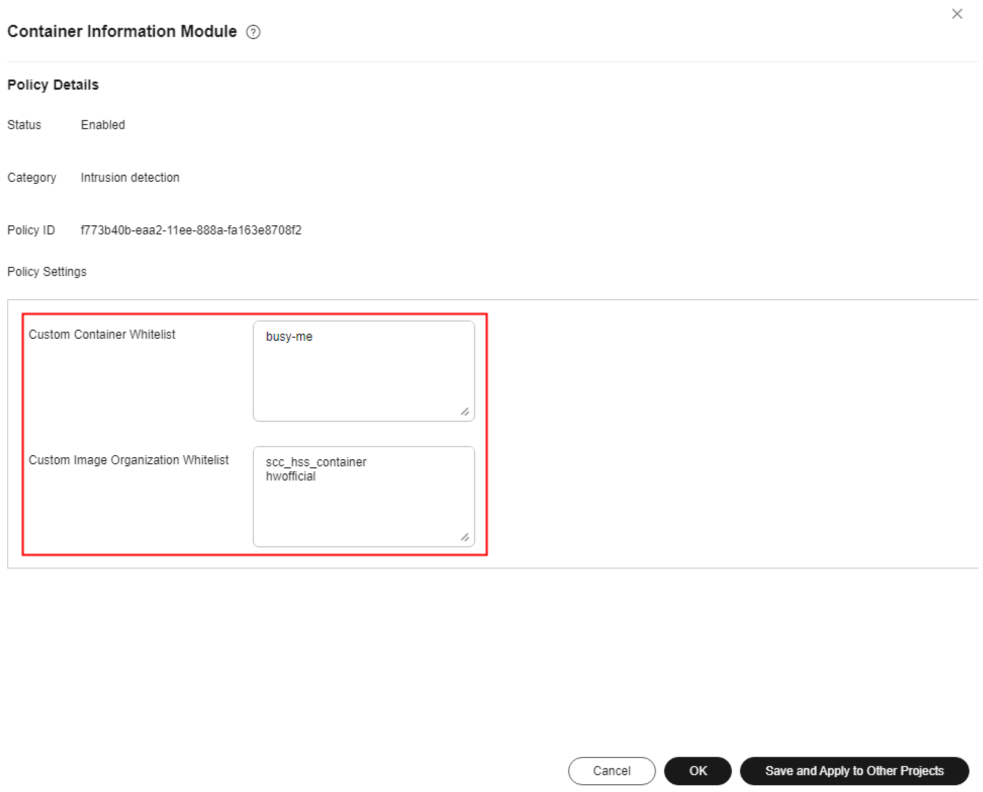
**Step 3** In the navigation pane, choose **Security Operations** > **Policies**.

**Step 4** Select the container policy group corresponding to the server and click the policy group name. The policy group details page is displayed.

**Step 5** Click the name of a **Container Information Module** policy. On the policy details page that is displayed, configure the whitelist.

You can configure the container and organization whitelist as required.

**Figure 13-8** Container information module policy



Container Information Module

Policy Details

Status Enabled

Category Intrusion detection

Policy ID f773b40b-eaa2-11ee-888a-fa163e8708f2

Policy Settings

Custom Container Whitelist: busy-me

Custom Image Organization Whitelist: scc_hss_container
hwofficial

**Table 13-7** Container information collection whitelist parameters

| Parameter | Example Value | Description |
|---|---|---|
| Custom Container Whitelist | **busy-me** | Enter the name of the **container** for which HSS alarms are not generated.<br>● Simple names of containers can be configured based on Docker. HSS automatically performs fuzzy match. Other containers perform exact match based on their names.<br>● Each container name needs to be on a separate line. Up to 100 whitelist items are allowed. |
| Custom image organization whitelist | **scc_hss_container**<br>**hwofficial** | Enter the organization name that can be used to prevent HSS alarms.<br>Each organization name needs to be on a separate line. Up to 100 whitelist items are allowed. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Container Process Whitelist

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

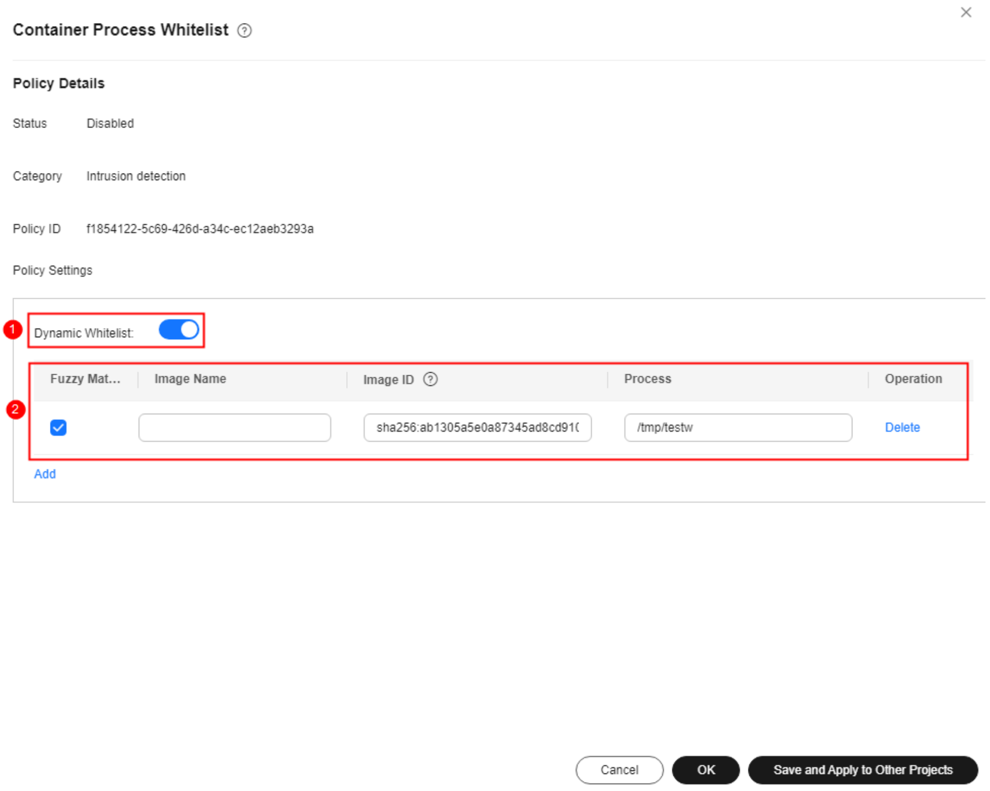
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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

**Step 4** Select the container policy group corresponding to the server and click the policy group name. The policy group details page is displayed.

**Step 5** Click the name of a **Container Process Whitelist** policy. On the policy details page, configure the container process whitelist.

**Figure 13-9** Container process whitelist policy



Container Process Whitelist ⓘ

Policy Details

| | |
|---|---|
| Status | Disabled |
| Category | Intrusion detection |
| Policy ID | f1854122-5c69-426d-a34c-ec12aeb3293a |

Policy Settings

1 Dynamic Whitelist: ●

2

| Fuzzy Mat... | Image Name | Image ID ⓘ | Process | Operation |
|---|---|---|---|---|
| ☑ | | sha256:ab1305a5e0a87345ad8cd91( | /tmp/testw | Delete |

**Table 13-8** Container process whitelist parameters

| Parameter ID in Figure 13-9 | Parameter | | Example Value | Description |
|---|---|---|---|---|
| ① | Dynamic Whitelist | | ● | Enable the dynamic whitelist **Figure 13-9**. HSS uses the following mechanism to detect container processes: By default, HSS uses the single-process model. That is, the container runs only the process command line configured in the container startup parameter. When a container is started, HSS automatically identifies the entrypoint configuration of the container and identifies the main process based on the entrypoint. If a process other than the main process is running during the container running, an alarm is generated. |
| ② | Whitelist | Fuzzy Match | **Select it.** | Indicates whether to enable fuzzy match for the target process path. |
| | | Image Name | - | Enter the name of the image to which the process belongs.<br>Enter either the image name or image ID. |
| | | Image ID | **sha256:ab1305a5e0a87345ad8cd91015990b7c34fb7a7e682266937872cefc9eb36671** | Enter the ID of the image to which the process belongs.<br>Enter either the image name or image ID. |
| | | Process | **/tmp/testw** | Enter the path of the process that does not need to be checked. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Fileless Attack Detection

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

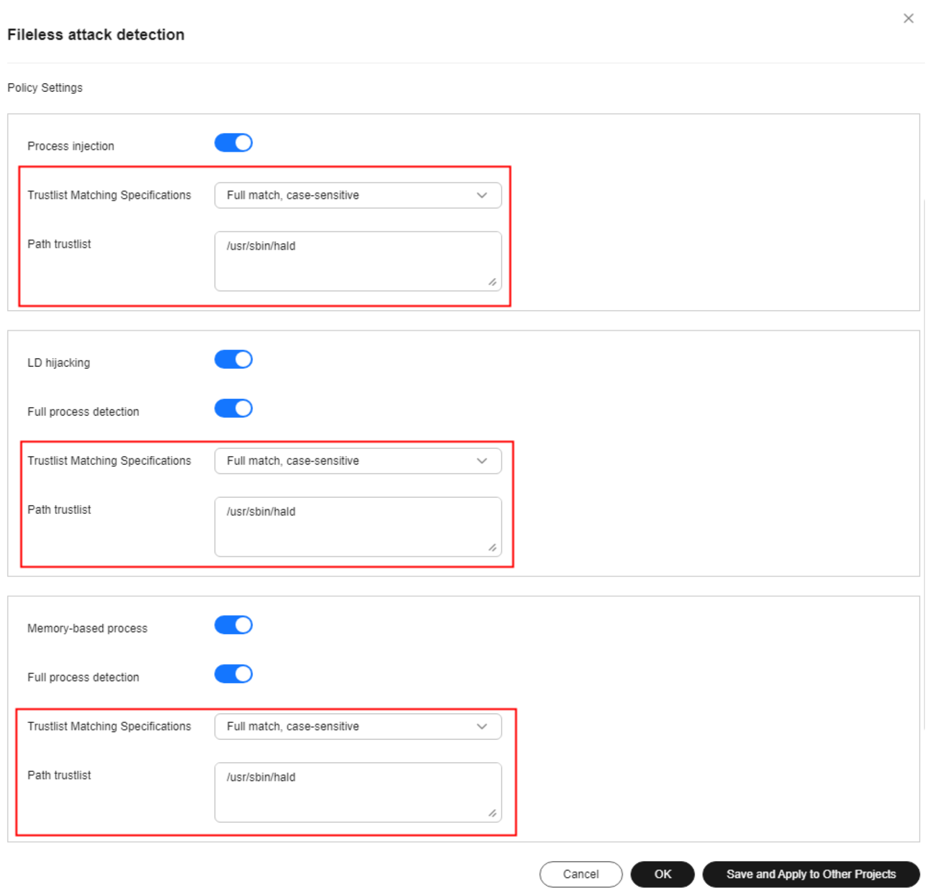
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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

**Step 4** Locate the policy group of the edition corresponding to the server and click the policy group name.

**Step 5** Click the name of a **Fileless Attack Detection** policy. On the policy details page that is displayed, set whitelist.

**Figure 13-10** Fileless attack detection policy



Fileless attack detection

Policy Settings

Process injection: ●

Trustlist Matching Specifications: Full match, case-sensitive

Path trustlist: /usr/sbin/hald

LD hijacking: ●

Full process detection: ●

Trustlist Matching Specifications: Full match, case-sensitive

Path trustlist: /usr/sbin/hald

Memory-based process: ●

Full process detection: ●

Trustlist Matching Specifications: Full match, case-sensitive

Path trustlist: /usr/sbin/hald

**Table 13-9** Parameters of the policy for fileless attack detection

| Parameter | Example Value | Description |
|---|---|---|
| Trustlist matching specifications | **Full match, case sensitive** | Path whitelist matching rule. Click ⌄ to select a whitelist matching rule. The options are as follows:<br>● Full match, case sensitive<br>● Full match, case-insensitive<br>● Fuzzy matching |

| Parameter | Example Value | Description |
|---|---|---|
| Path trustlist | **/usr/sbin/hald** | Enter paths that do not need to be detected for **Process injection**, **LD hijacking**, or **Memory-based process**. Separate multiple paths by line breaks. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## File Protection

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

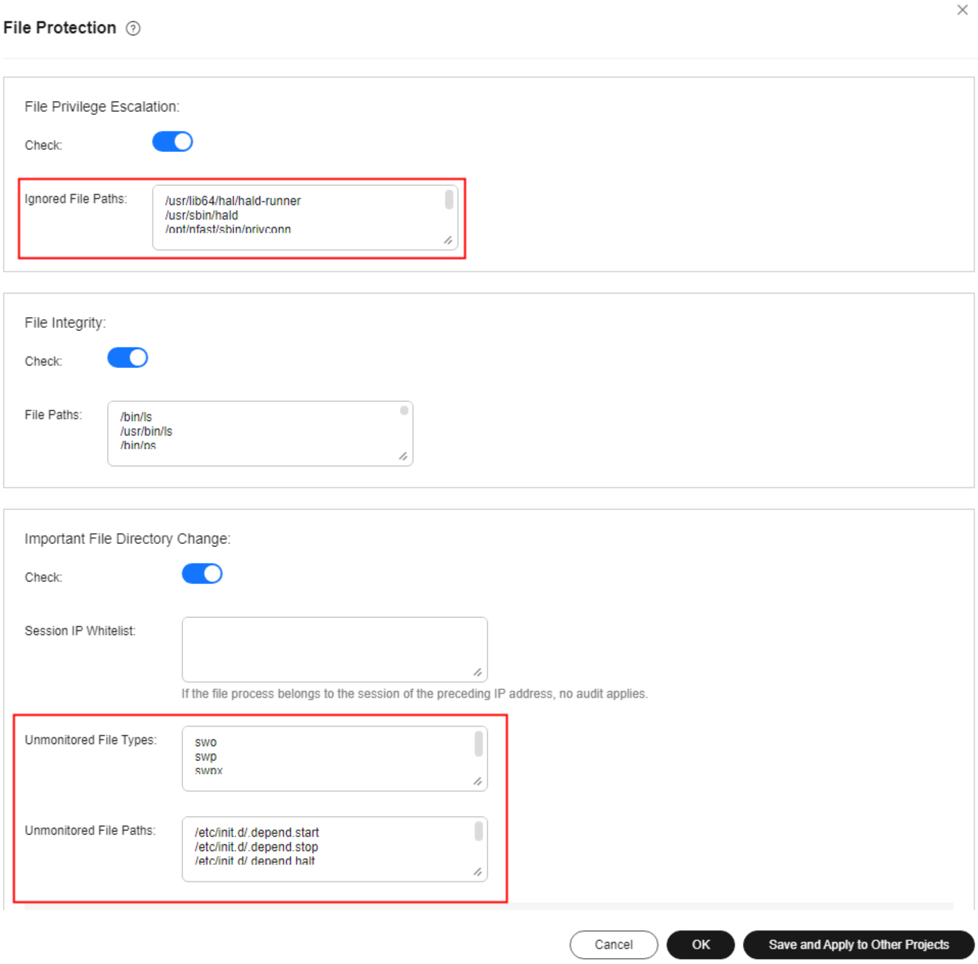
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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

**Step 4** Select the policy group of the corresponding protection version. The policy group details page is displayed.

**Step 5** Click the name of a target policy. On the details page that is displayed, configure the types or paths of files that can be ignored.

**Figure 13-11** File protection policy



File Protection

File Privilege Escalation:

Check: ●

Ignored File Paths:

```
/usr/lib64/hal/hald-runner
/usr/sbin/hald
/opt/nfast/sbin/privconn
```

File Integrity:

Check: ●

File Paths:

```
/bin/ls
/usr/bin/ls
/bin/ps
```

Important File Directory Change:

Check: ●

Session IP Whitelist:

If the file process belongs to the session of the preceding IP address, no audit applies.

Unmonitored File Types:

```
swo
swp
swpx
```

Unmonitored File Paths:

```
/etc/init.d/.depend.start
/etc/init.d/.depend.stop
/etc/init.d/.depend.halt
```

**Table 13-10** Parameter description

| Category | Parameter | Example Value | Description |
|---|---|---|---|
| File Privilege Escalation | Ignored File Paths | **/usr/lib64/hal/hald-runner**<br>**/usr/sbin/hald**<br>**/opt/nfast/sbin/privconn**<br>**/usr/sbin/dhclient**<br>**/usr/sbin/tcpdump** | Enter the path of the file to be ignored. Start the path with a slash (/) and do not end it with a slash (/). Each path occupies a line. No spaces are allowed between path names. |
| Important File Directory Change | Unmonitored File Types | **swo**<br>**swp**<br>**swpx**<br>**lck** | Enter the suffix of the unmonitored file type. Multiple file types are separated by line breaks. |

| Category | Parameter | Example Value | Description |
|---|---|---|---|
| | Unmonitored File Paths | **/etc/init.d/.depend.start**<br>**/etc/init.d/.depend.stop**<br>**/etc/init.d/.depend.halt**<br>**/etc/init.d/.depend.boot**<br>**/var/spool/cron/sed*** | Enter the path of the file to be ignored. Start the path with a slash (/) and do not end it with a slash (/). Each path occupies a line. No spaces are allowed between path names. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## HIPS Detection

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

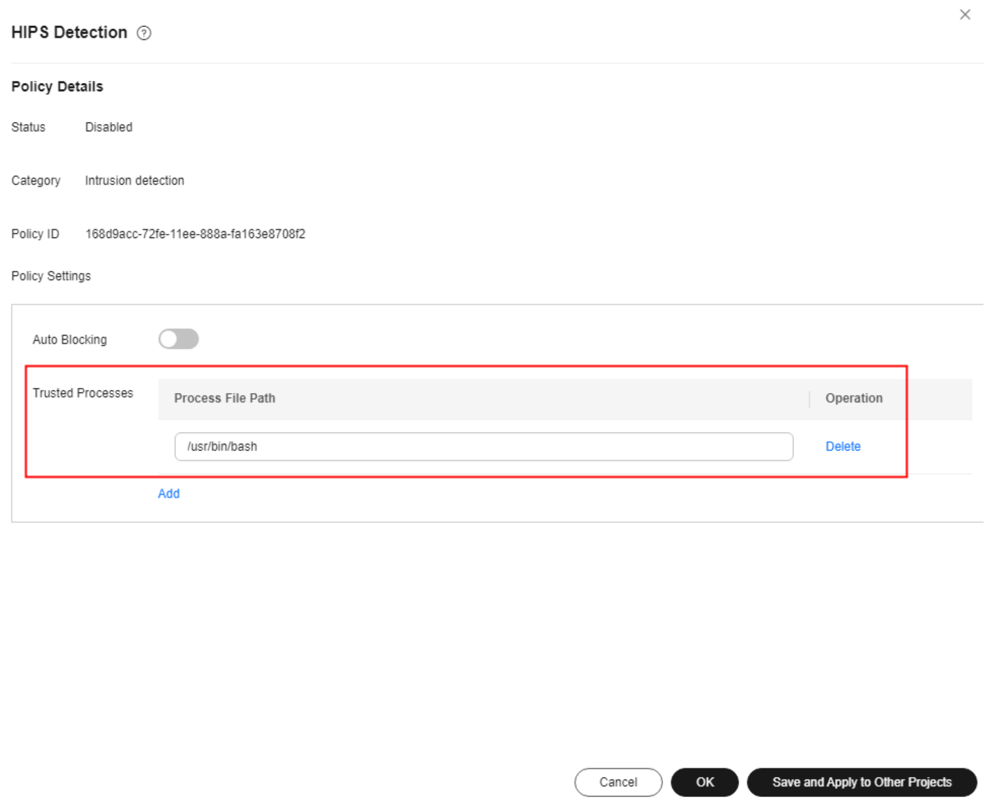
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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

**Step 4** Select the policy group of the corresponding protection version. The policy group details page is displayed.

**Step 5** Click the name of a HIPS detection policy. On the details page that is displayed, configure the trusted process.

**Figure 13-12** HIPS detection policy



HIPS Detection

Policy Details

Status Disabled

Category Intrusion detection

Policy ID 168d9acc-72fe-11ee-888a-fa163e8708f2

Policy Settings

Auto Blocking

Trusted Processes

| Process File Path | Operation |
|---|---|
| /usr/bin/bash | Delete |

**Table 13-11** Parameters description of the HIPS detection policy whitelist

| Parameter | Example Value | Description |
|---|---|---|
| Process File Path | **/usr/bin/bash** | Add the full path of the trusted process. You can click **Add** to add a path and click **Delete** to delete it. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Login Security Check

The login security detection policy not only generates alarms for brute-force attacks, but also blocks brute-force attack IP addresses. If you only add alarms to the login alarm whitelist, subsequent alarms can be avoided, but the trusted IP addresses are blocked. You can set trusted IP addresses in the login security detection policy to avoid alarms and blocking.

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

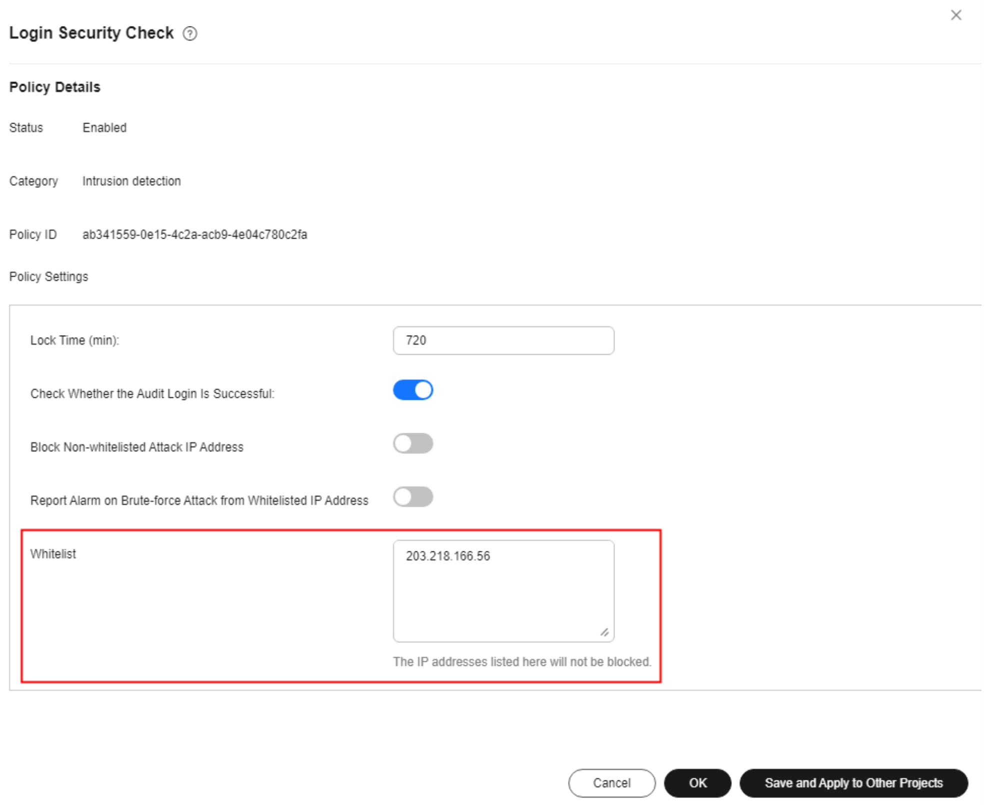
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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

**Step 4** Select the policy group of the corresponding protection version. The policy group details page is displayed.

**Step 5** Click the name of the login security detection policy. On the details page that is displayed, configure trusted IP addresses.

**Figure 13-13** Login security detection policy



Login Security Check

Policy Details

Status Enabled

Category Intrusion detection

Policy ID ab341559-0e15-4c2a-acb9-4e04c780c2fa

Policy Settings

Lock Time (min): 720

Check Whether the Audit Login Is Successful: ●

Block Non-whitelisted Attack IP Address ○

Report Alarm on Brute-force Attack from Whitelisted IP Address ○

Whitelist 203.218.166.56

The IP addresses listed here will not be blocked.

**Table 13-12** Parameter description

| Parameter | Example Value | Description |
|---|---|---|
| Report Alarm on Brute-force Attack from Whitelisted IP Address | ○ | Specifies whether an alarm is generated when brute force cracking occurs on an IP address in the whitelist.<br>○ indicates that no alarm is generated. |

| Parameter | Example Value | Description |
|---|---|---|
| Whitelist | **203.218.166.56** | After an IP address is added to the whitelist, HSS does not block brute force attacks from the IP address in the whitelist.<br>A maximum of 50 IP addresses or network segments can be added to the whitelist. Both IPv4 and IPv6 addresses are supported. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Malicious File Detection

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

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

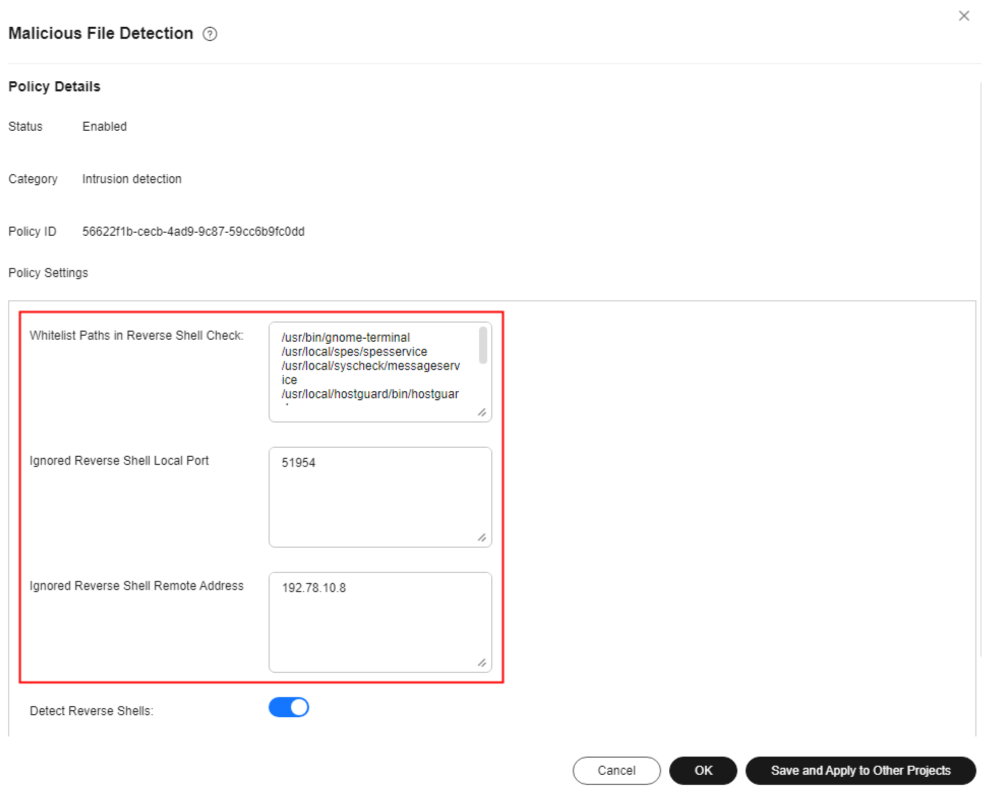
**Step 3** In the navigation pane, choose **Security Operations** > **Policies**.

**Step 4** Select the policy group of the corresponding protection version. The policy group details page is displayed.

**Step 5** Click the name of the malicious file detection policy. On the details page that is displayed, configure the content to be ignored.

You only need to configure the content to be ignored.

**Figure 13-14** Malicious file detection policy



Malicious File Detection

Policy Details

Status Enabled

Category Intrusion detection

Policy ID 56622f1b-cecb-4ad9-9c87-59cc6b9fc0dd

Policy Settings

Whitelist Paths in Reverse Shell Check: /usr/bin/gnome-terminal /usr/local/spes/spesservice /usr/local/syscheck/messageservice /usr/local/hostguard/bin/hostguar

Ignored Reverse Shell Local Port 51954

Ignored Reverse Shell Remote Address 192.78.10.8

Detect Reverse Shells: ●

**Table 13-13** Parameter description

| Parameter | Example Value | Description |
|---|---|---|
| Whitelist Paths in Reverse Shell Check | **/usr/bin/gnome-terminal**<br>**/usr/local/spes/spesservice**<br>**/usr/local/syscheck/messageservice**<br>**/usr/local/hostguard/bin/hostguard** | Enter the whitelist path in reverse shell check.<br>Start with a slash (/) and end with no slashes (/). Occupy a separate line and cannot contain spaces. |
| Ignored Reverse Shell Local Port | **51954** | Enter the ignored reverse shell local port. Separate multiple ports with commas (,). |

| Parameter | Example Value | Description |
|---|---|---|
| Ignored Reverse Shell Remote Address | **192.78.10.8** | Enter the ignored remote IP address or network segment in reverse shell detection. Use commas (,) to separate multiple IP addresses or network segments. Enter an IPv4 or IPv6 address.<br>For example:<br>● IPv4 address: 192.78.10.3<br>● IPv4 network segment: 192.78.10.0/255.255.255.0 or 192.78.10.0/24<br>● IPv6 address: 2001:0db8:86a3:08d3:1319:8a2e:0370:7344<br>● IPv6 network segment: 234e:0:4567 3d/ffff ffff:ffff:ffff::0 or 2001:db8:832:11::/64 |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Port Scan Detection

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

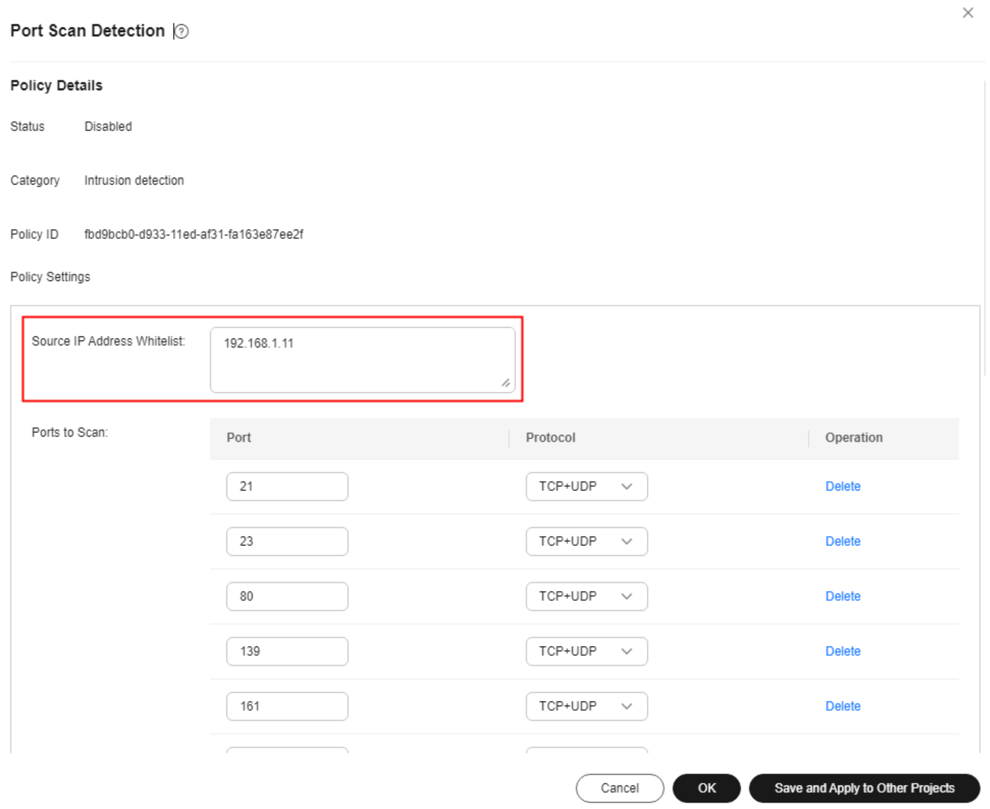
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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

**Step 4** Select the policy group of the corresponding protection version. The policy group details page is displayed.

**Step 5** Click the name of the port scan detection policy. On the details page that is displayed, configure the source IP address whitelist.

**Figure 13-15** Port scan detection policy



Port Scan Detection

Policy Details

Status Disabled

Category Intrusion detection

Policy ID fbd9bcb0-d933-11ed-af31-fa163e87ee2f

Policy Settings

Source IP Address Whitelist: 192.168.1.11

Ports to Scan:

| Port | Protocol | Operation |
|---|---|---|
| 21 | TCP+UDP | Delete |
| 23 | TCP+UDP | Delete |
| 80 | TCP+UDP | Delete |
| 139 | TCP+UDP | Delete |
| 161 | TCP+UDP | Delete |

**Table 13-14** Port scan detection policy whitelist parameters

| Parameter | Example Value | Description |
|---|---|---|
| Source IP Address Whitelist | **192.168.1.11** | Scan for ignored source IP addresses. IP addresses or masks are supported. Use commas (,) to separate multiple IP addresses or masks. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Root Privilege Escalation

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

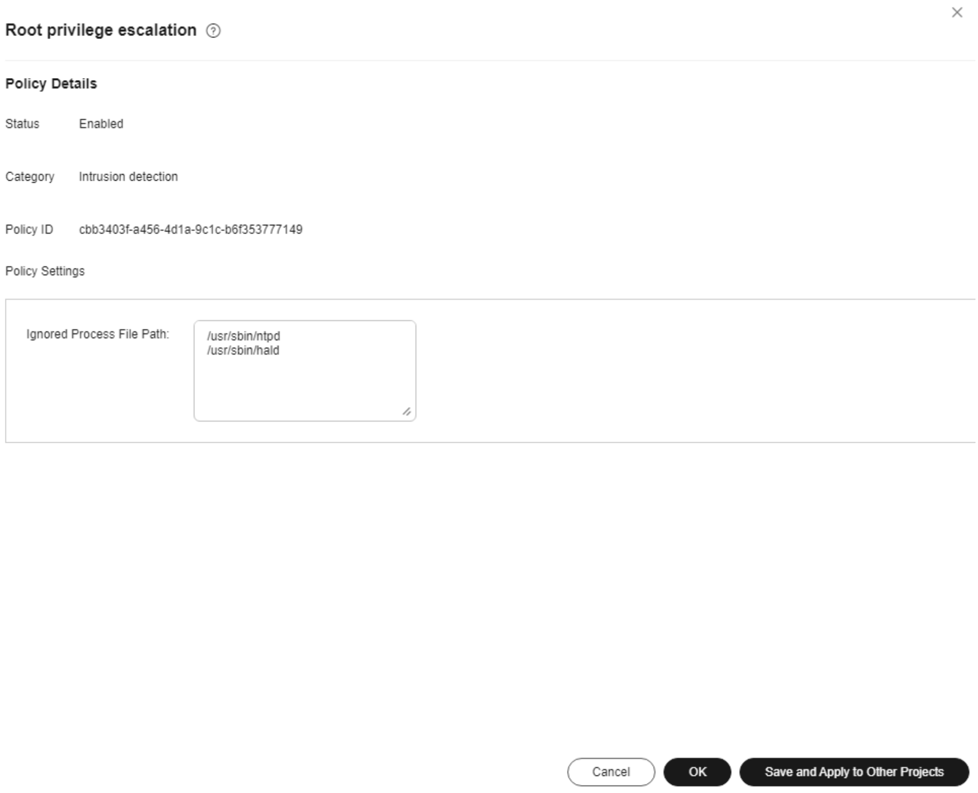
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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

**Step 4** Select the policy group of the corresponding protection version. The policy group details page is displayed.

**Step 5** Click the name of the root privilege escalation policy. On the details page that is displayed, configure the path of the ignored process file.

**Figure 13-16** Root privilege escalation policy



Root privilege escalation

Policy Details

Status Enabled

Category Intrusion detection

Policy ID cbb3403f-a456-4d1a-9c1c-b6f353777149

Policy Settings

Ignored Process File Path:
/usr/sbin/ntpd
/usr/sbin/hald

**Table 13-15** Parameters description of the root privilege escalation policy whitelist

| Parameter | Example Value | Description |
|---|---|---|
| Ignored Process File Path | **/usr/sbin/ntpd**<br>**/usr/sbin/hald** | Set the ignored process file path.<br>Start with a slash (/) and end with no slashes (/). Occupy a separate line and cannot contain spaces. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Real-time Process

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

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

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

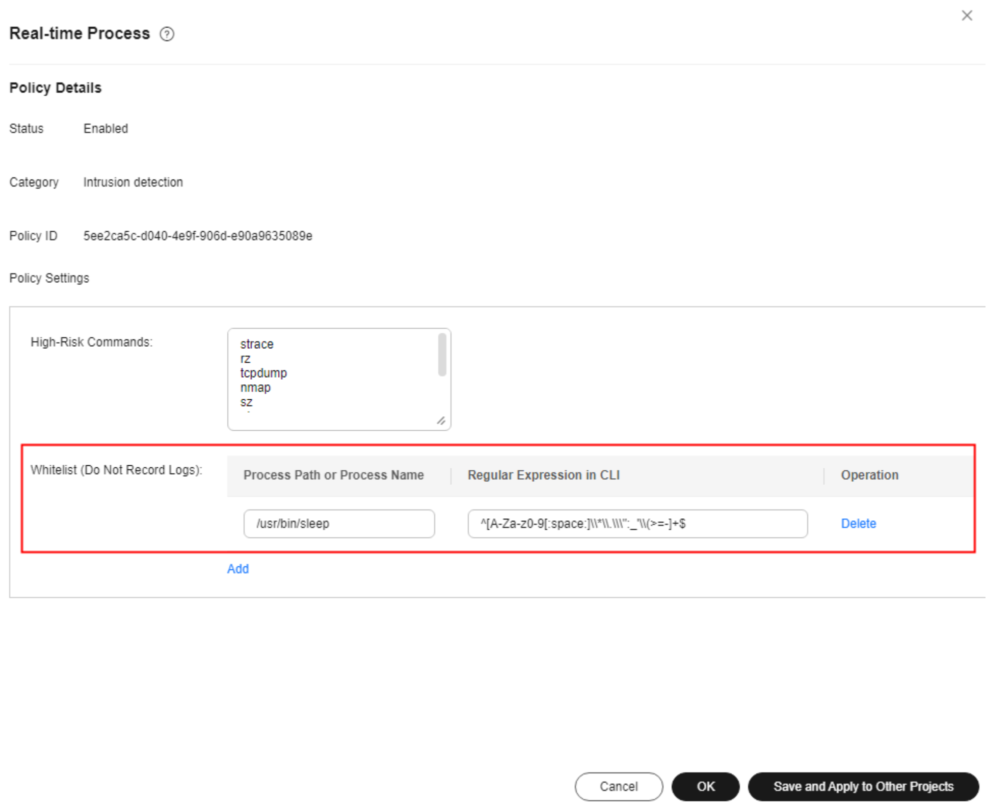
**Step 4** Select the policy group of the corresponding protection version. The policy group details page is displayed.

**Step 5** Click the name of the real-time process policy. The policy details page is displayed.

**Step 6** In the **Whitelist** area, click **Add** to add a whitelist text box.

**Step 7** Set whitelist parameters as prompted.

**Figure 13-17** Real-time process policy



Real-time Process

Policy Details

Status Enabled

Category Intrusion detection

Policy ID 5ee2ca5c-d040-4e9f-906d-e90a9635089e

Policy Settings

High-Risk Commands:
strace
rz
tcpdump
nmap
sz

Whitelist (Do Not Record Logs):

| Process Path or Process Name | Regular Expression in CLI | Operation |
|---|---|---|
| /usr/bin/sleep | ^[A-Za-z0-9[:space:]*\\.\\\":_"\\(>=-]+$ | Delete |

**Table 13-16** Parameters of the real-time process policy whitelist

| Parameter | Example Value | Description |
|---|---|---|
| Process Path or Process Name | **/usr/bin/sleep** | Add paths or program names that are allowed or ignored during detection. |

| Parameter | Example Value | Description |
|---|---|---|
| Command Expression in CLI | **^[A-Za-z0-9[:space:]\\*\\.\\\":_'\\(>=-]+$** | Enter the regular expression of the whitened command line.<br>This parameter is optional. |

**Step 8** Confirm the information and click **OK**.

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**

## Rootkit Detection

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

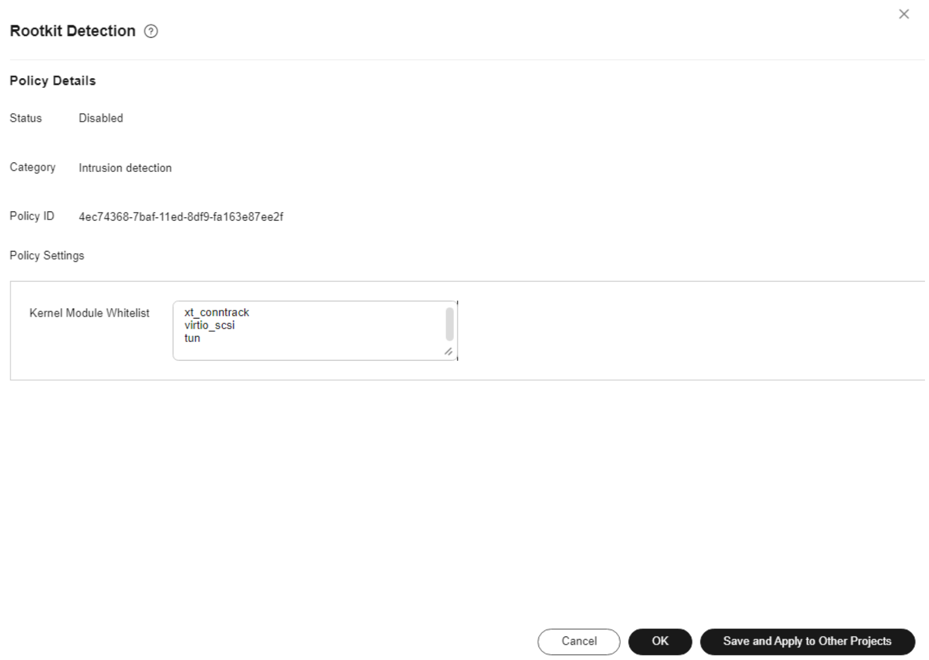
**Step 2** In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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

**Step 4** Select the policy group of the corresponding protection version. The policy group details page is displayed.

**Step 5** Click the name of the rootkit detection policy. On the details page that is displayed, configure the kernel module whitelist.

**Figure 13-18** Rootkit detection policy



Rootkit Detection

Policy Details

Status Disabled

Category Intrusion detection

Policy ID 4ec74368-7baf-11ed-8df9-fa163e87ee2f

Policy Settings

Kernel Module Whitelist
xt_conntrack
virtio_scsi
tun

**Table 13-17** Parameters description of the rootkit detection policy whitelist

| Parameter | Example Value | Description |
|---|---|---|
| Kernel Module Whitelist | **xt_conntrack**<br>**virtio_scsi**<br>**tun** | Add the kernel modules that can be ignored during the detection.<br>Up to 10 kernel modules can be added. Multiple modules are separated by line breaks. |

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

If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same version.

**----End**