Host Security Service (HSS)

Best Practices

Issue	04
Date	2025-01-06

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

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

Contents

1 Suggestions on How to Fix Official Disclosed Vulnerabilities Provided by HSS

1.1 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.

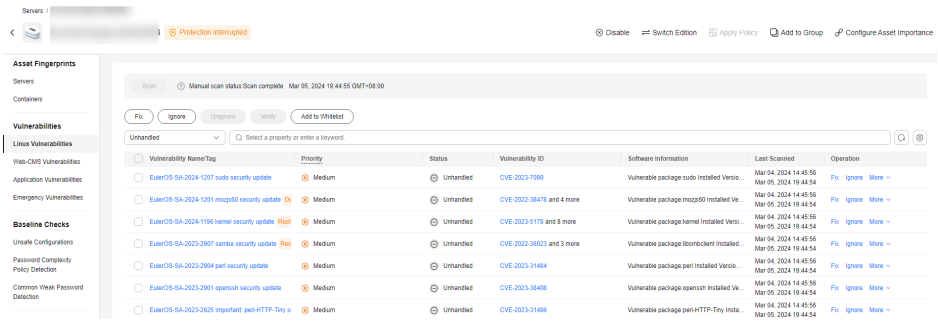
Download address: **https://github.com/git/git/releases**

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 1-1 Manually starting a vulnerability scan



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.

1.2 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.

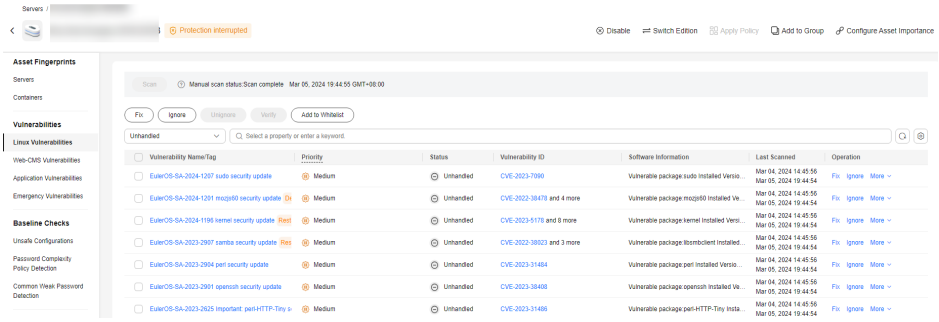
Suggestion

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**.

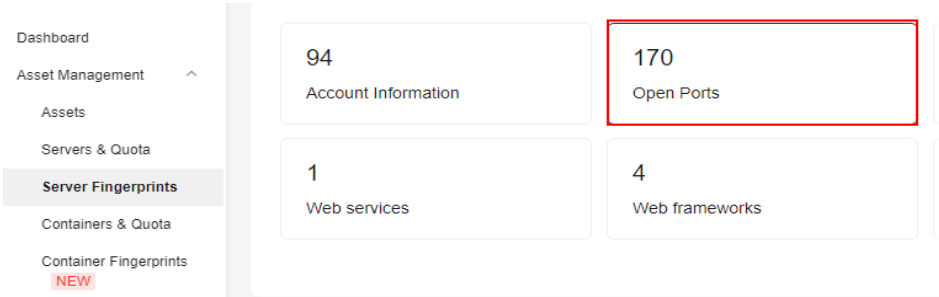
  Figure 1-2 Manually starting a vulnerability scan



- Check whether ports 4505 and 4506 are enabled on the server.

  If ports **4505** and **4506** are enabled, you are advised to disable them or enable them only for trusted objects. For details, see **Checking Open Ports**.

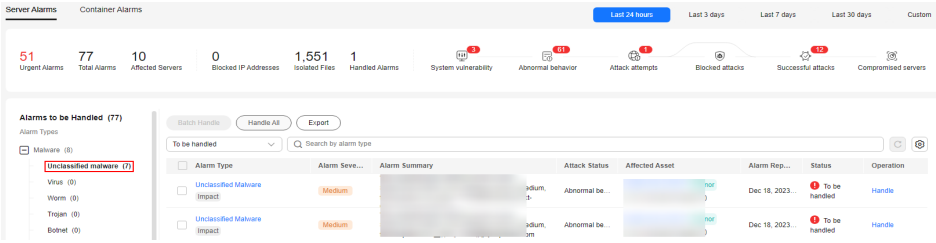
  Figure 1-3 Server fingerprints



- Check for, isolate, and kill Trojans.

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

Figure 1-4 Managing the isolated files



1.3 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.

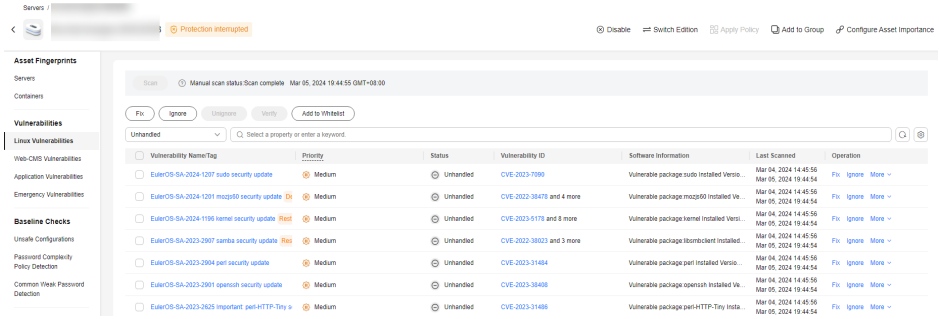
- **https://www.debian.org/security/2020/dsa-4661**
- **https://security.gentoo.org/glsa/202004-10**
- **https://lists.suse.com/pipermail/sle-security-updates/2020-April/006722.html**

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 1-5 Manually starting a vulnerability scan



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

----End

1.4 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.

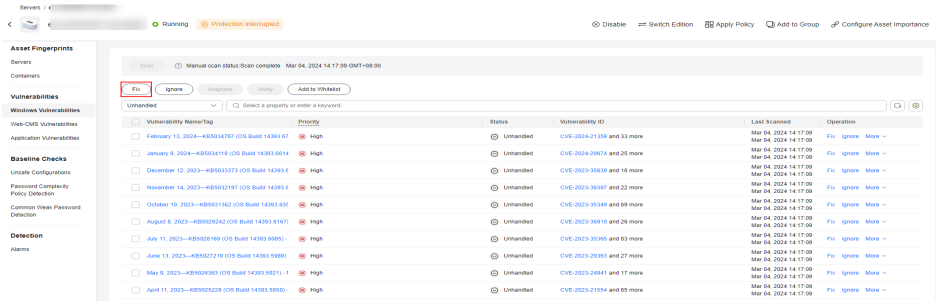
For details, see https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1020.

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 1-6 Manually starting a vulnerability scan



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

----End

1.5 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.

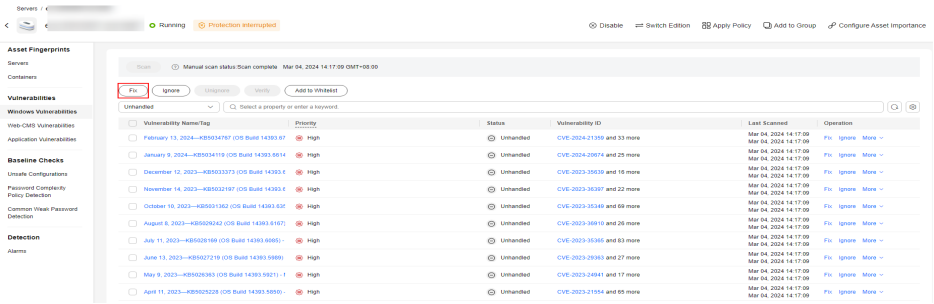
For details, see https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1027.

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 1-7 Manually starting a vulnerability scan



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

----End

1.6 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.

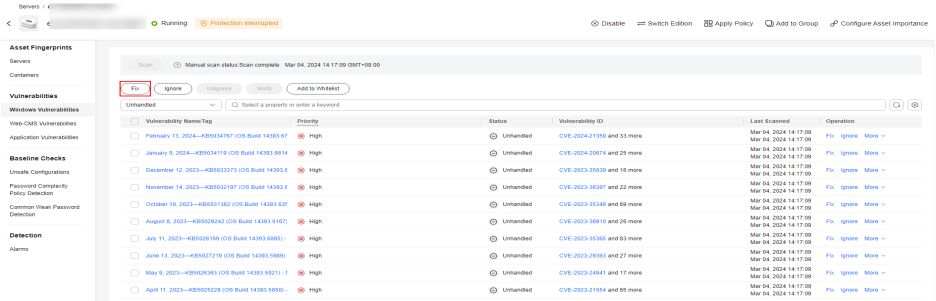
Step 1 Log in to the management console.

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 1-8 Manually starting a vulnerability scan



Step 5 Fix detected vulnerabilities according to the suggestion in the **Solution** column.

Step 6 Restart the fixed servers.

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

NOTE

You can also choose **Vulnerabilities** and click **Windows Vulnerabilities**, search for a vulnerability by its name, and then check and fix the vulnerability.

- Windows Server 2019: KB4534273
- Windows Server 2016: KB4534271

----End

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

2.1 Overview

Scenario

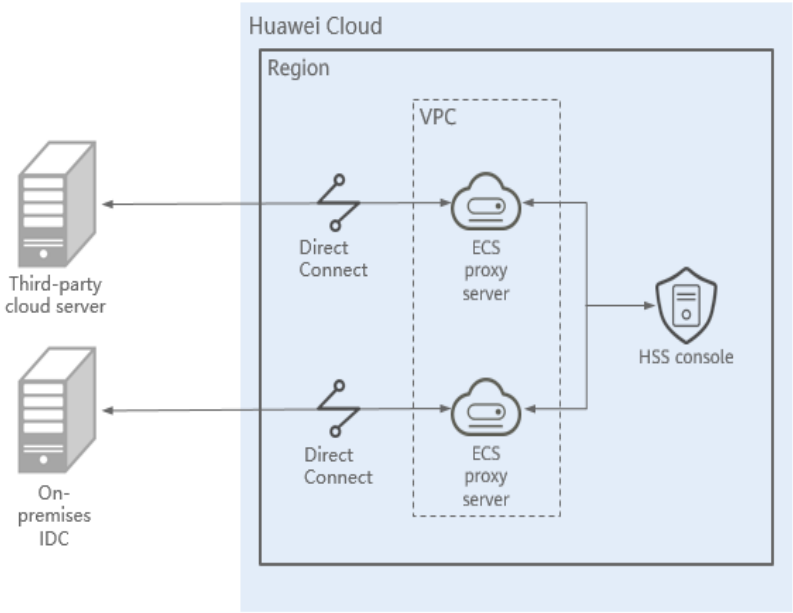
With the development of hybrid clouds, there is also a growing need for companies to perform unified security management of on- and off-cloud or hybrid clouds. HSS supports the access and management of third-party cloud servers and on-premises IDCs. Users are allowed to use the same security policies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

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 ConnectDirect 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)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 2-1 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.

2.2 Resources and Costs

The following table lists resources in this example.

Table 2-1 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**.

2.3 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.

2.4 Process

2.4.1 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 how to use Direct Connect to connect a third-party server to a VPC, see **Using Direct Connect to Connecting an On-premises Data Center to the Cloud**.

2.4.2 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

2.4.3 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.

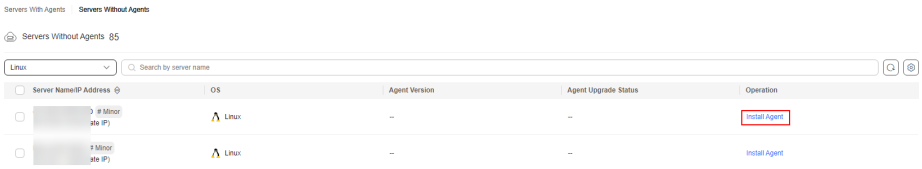
Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > HSS.

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 2-2 Installing an agent

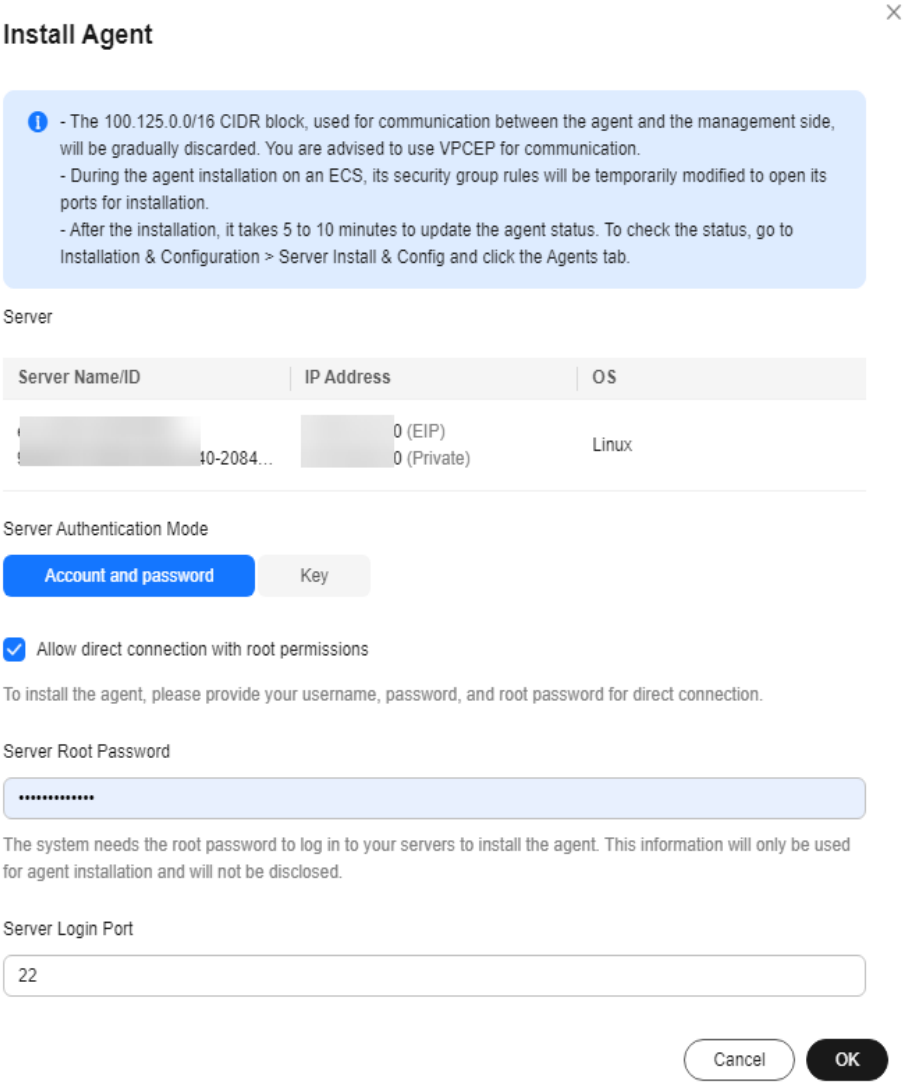


Step 7 Select and set the server verification information.

- **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 2-3 Enter the server verification information.



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

2.4.4 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 2-4 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 2-5 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 2-6 Installing Nginx (yum)

```
[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 2-7 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 2-8 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 ~]#
```

   - 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 2-9 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 2-10 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 2-11 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 2-12 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 2-13 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

2.4.5 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 2-14 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

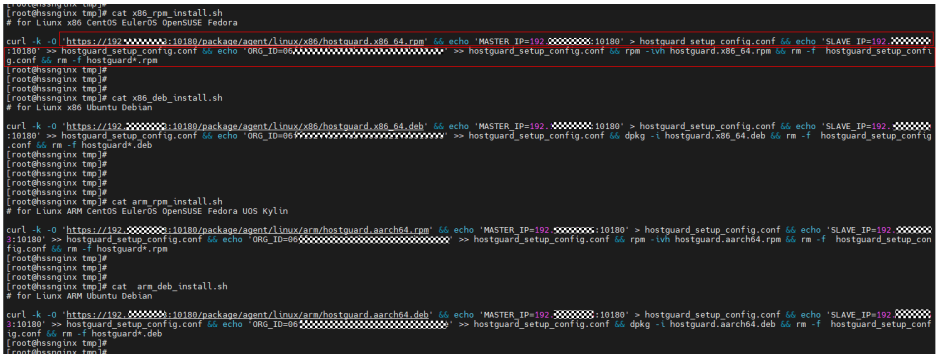
enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2`#g" *install.sh

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 2-15 Linux installation commands



----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

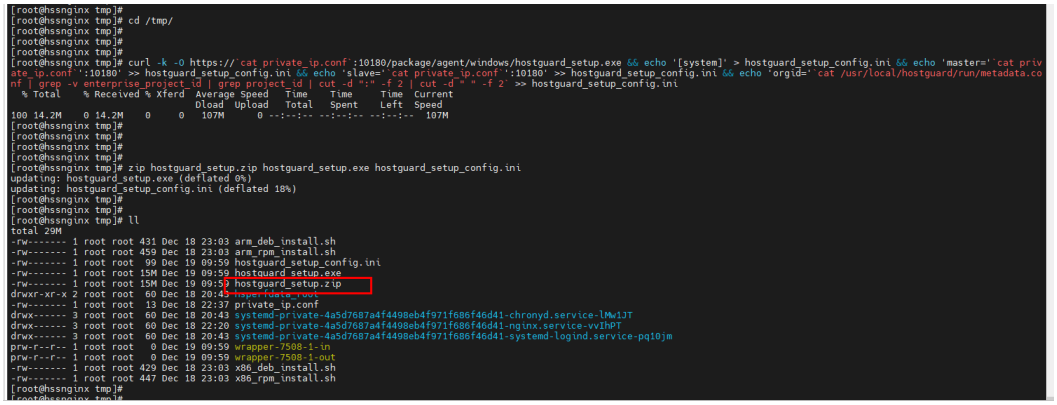
NOTE

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 2-16 Windows installation package



----End

2.4.6 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 2-17 Installing an agent

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

3 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.

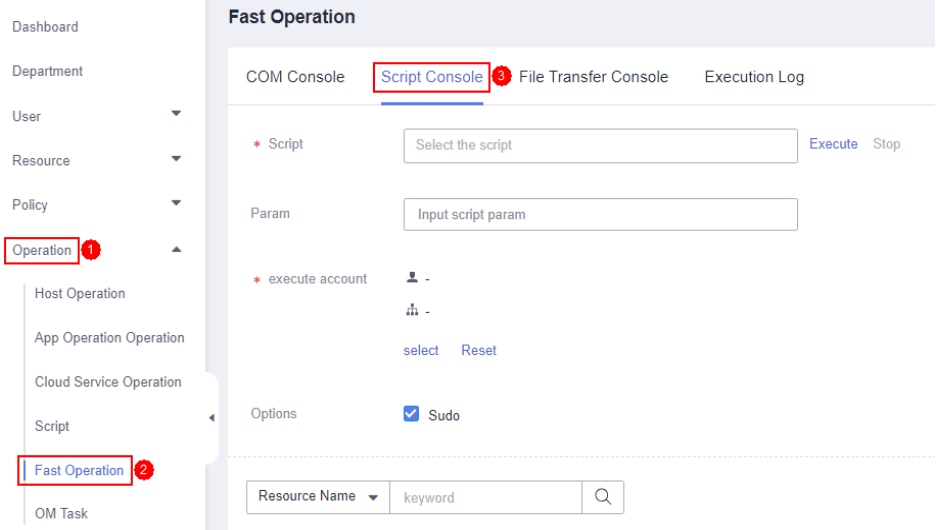
Procedure

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 3-1 Accessing the Script Console



Step 4 Configure script O&M information. **Script O&M parameters** describes the parameters.

Figure 3-2 Configuring script O&M information

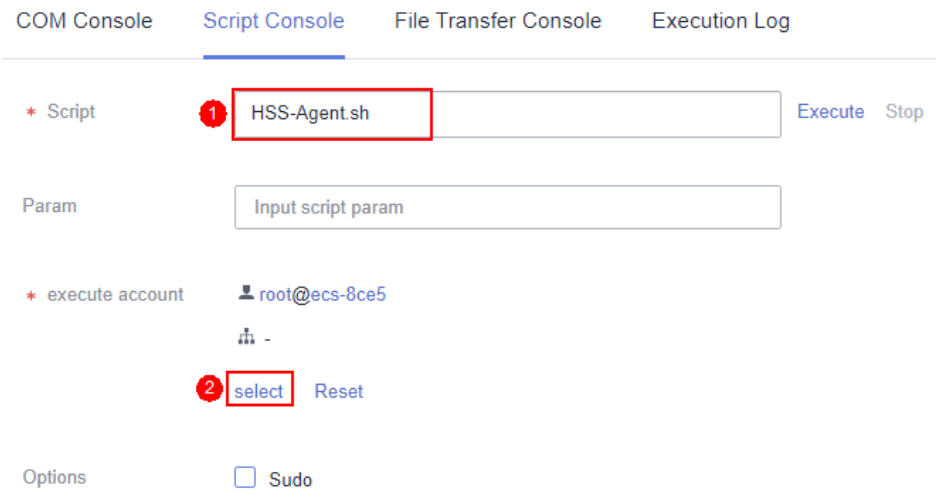


Table 3-1 Script O&M parameters

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**.

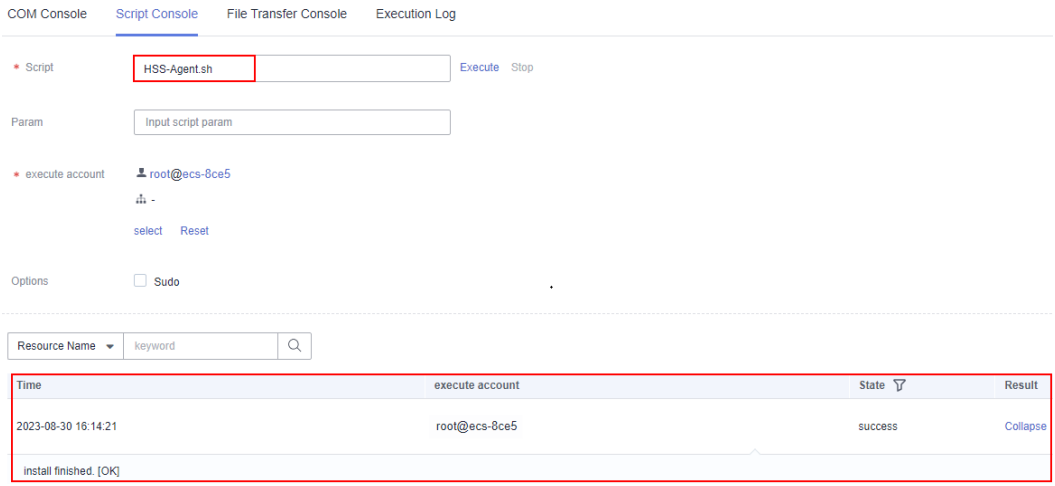
Step 5 Click **Execute**.

Figure 3-3 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 3-4 Successfully executed a script task

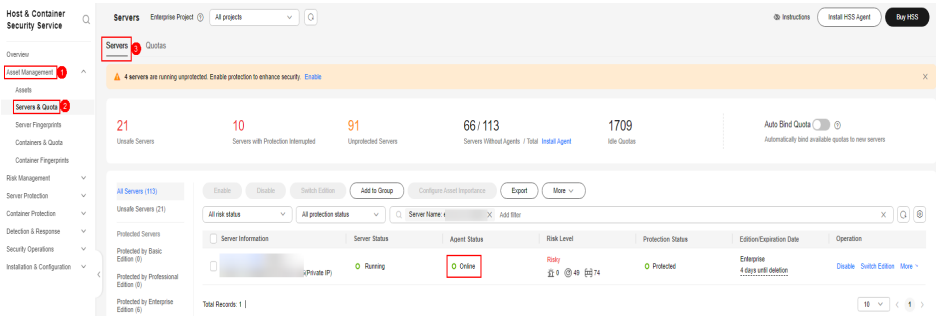


Step 7 On the HSS console, confirm the agent installation result.

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 3-5 Checking the agent status



----End

4 Using HSS to Improve Server Login Security

Scenario

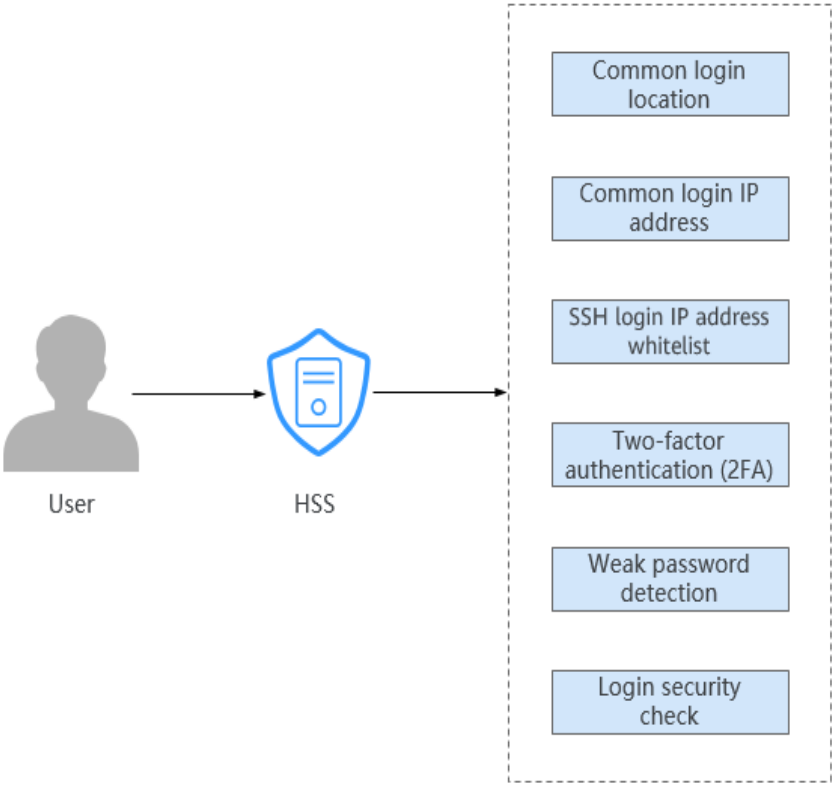
Account and password cracking are the most commonly used ways for attackers to intrude or attack servers. Enhancing login security is the first step to protect server security and ensure that services can run properly.

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 4-1 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.

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.

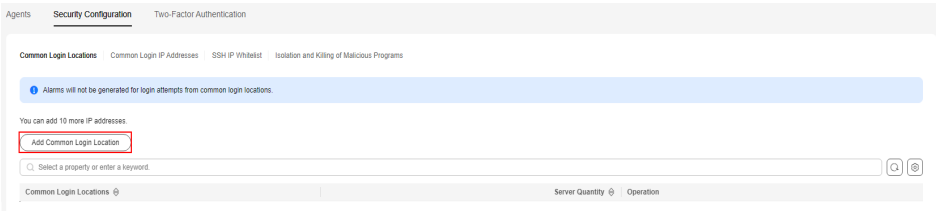
Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > HSS.

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**.

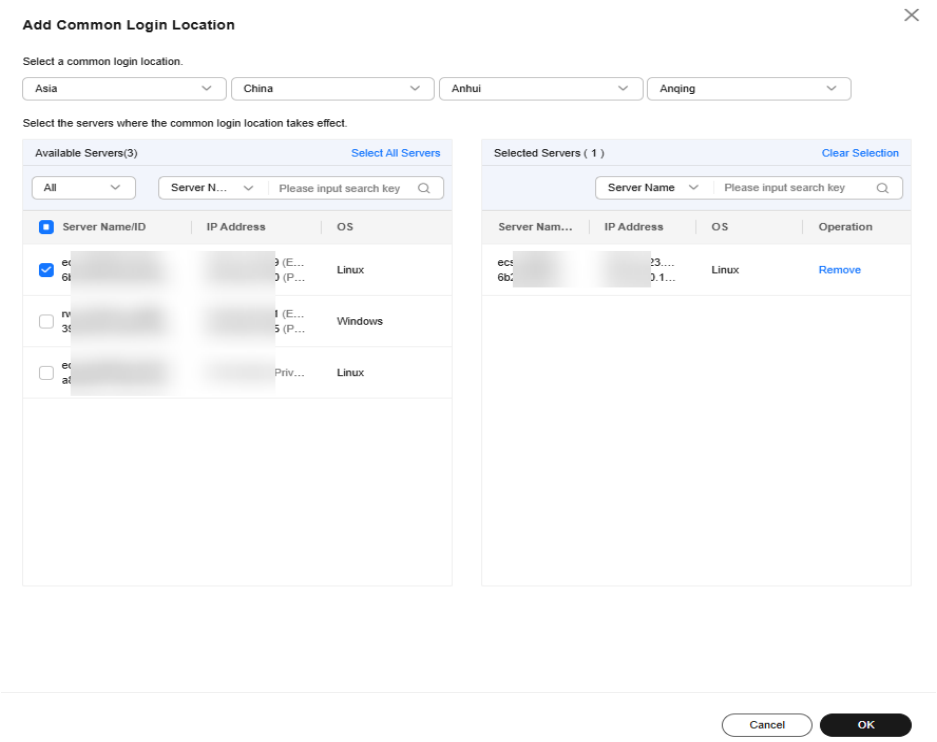
Figure 4-2 Adding a common login location



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 4-3 Configuring common login locations



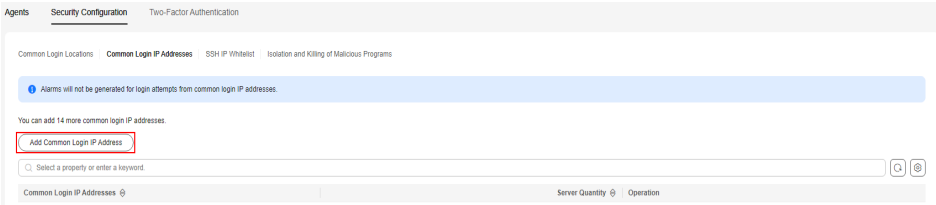
5. Return to the Common Login Locations sub-tab and check the added common login locations.

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 4-4 Adding a common login IP address

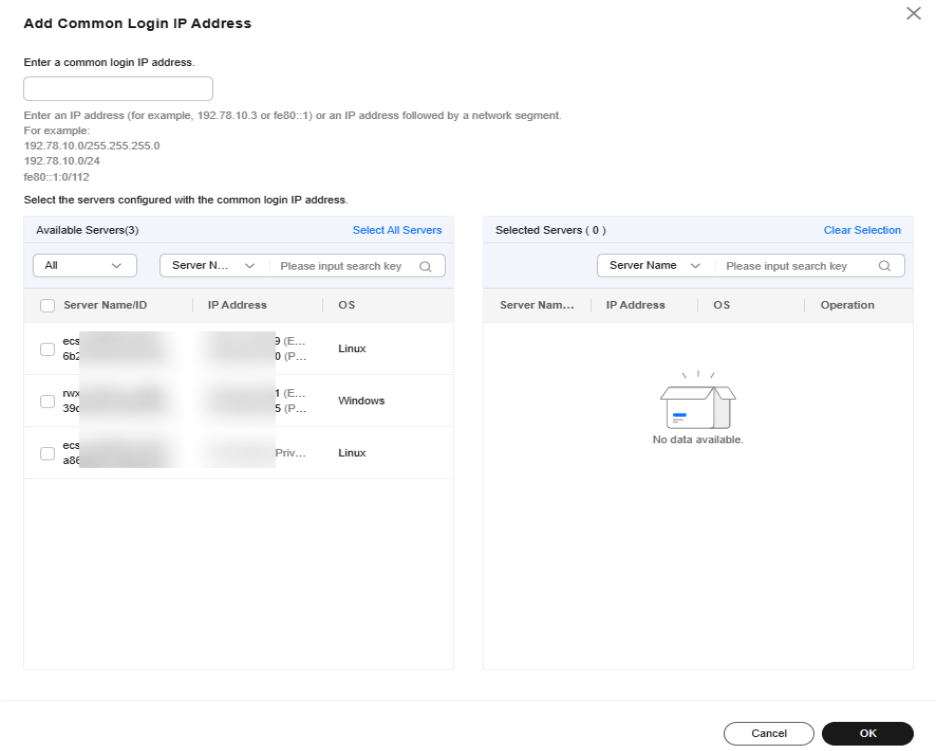


3. In the dialog box that is displayed, enter a common login IP address and select servers. Confirm the information and click **OK**.

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 4-5 Entering a common login IP address



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

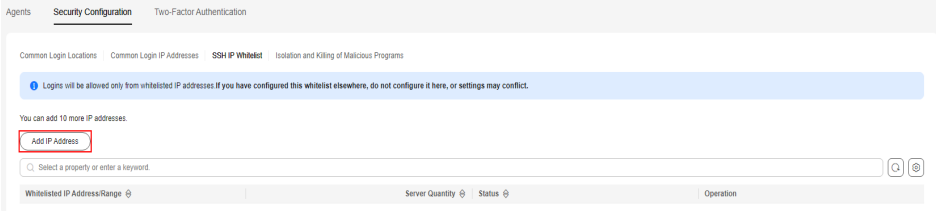
NOTE

- 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 4-6 Configuring an IP address whitelist

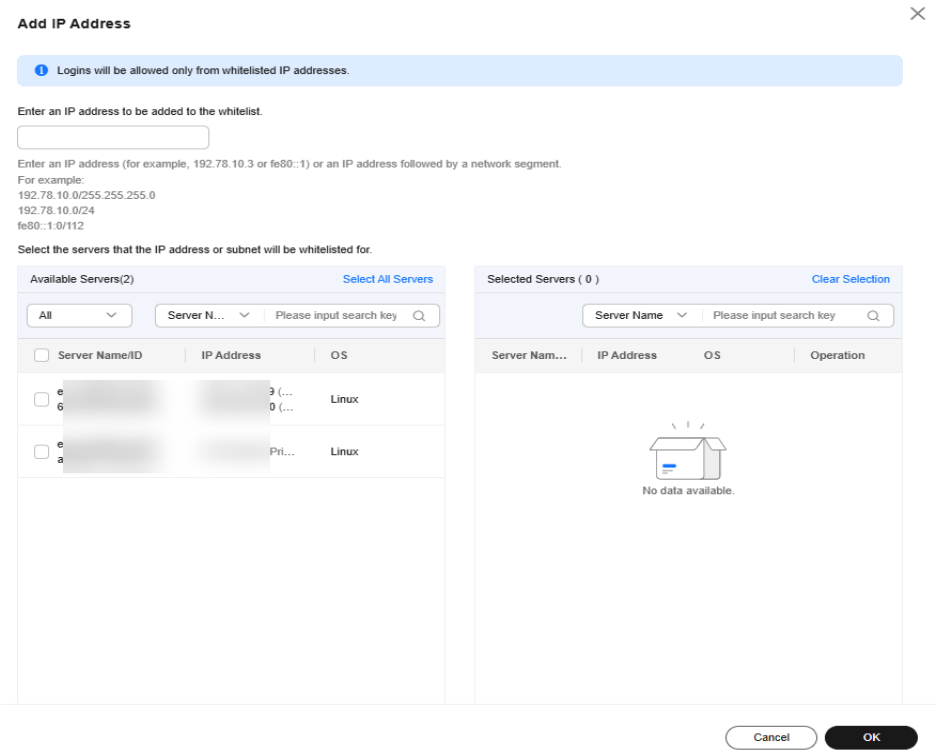


3. In the dialog box that is displayed, enter an IP address to be added to the whitelist and select servers. Confirm the information and click **OK**.

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 4-7 Entering an IP address



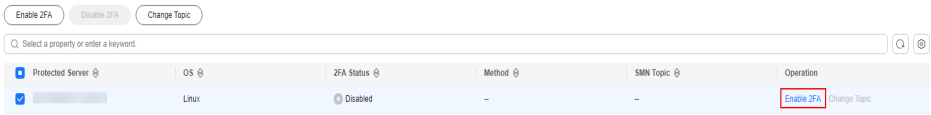
4. The **SSH IP Whitelist** sub-tab and check the added IP whitelist.

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 4-8 Enabling 2FA



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**.
     - During authentication, all the mobile numbers and email addresses specified in the topic will receive a verification SMS or email. You can delete mobile numbers and email addresses that do not need to receive verification messages.
   - **Verification code**

     Use the verification code you receive in real time for verification.
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 4-1**.

Table 4-1 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. Enter only one weak password per line. Up to 300 weak passwords can be added.	test123*

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 4-2**.

Figure 4-9 Modifying the security check policy

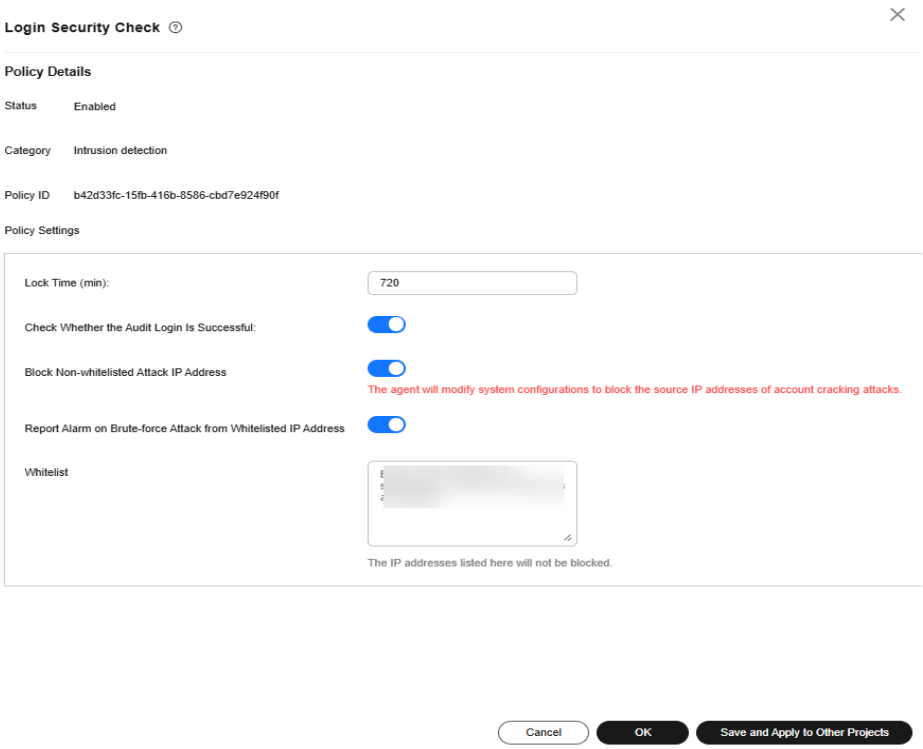


Table 4-2 Parameter description

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. ▪ : enabled ▪ : disabled
Block Non-whitelisted Attack IP Address	After this function is enabled, HSS blocks the login of brute force IP addresses (non-whitelisted IP addresses).
Report Alarm on Brute-force Attack from Whitelisted IP Address	– After this function is enabled, HSS generates alarms for brute force attacks from whitelisted IP addresses. ▪ : enabled ▪ : disabled

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

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

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

----End

5 Using HSS and CBR to Defend Against Ransomware

5.1 Overview

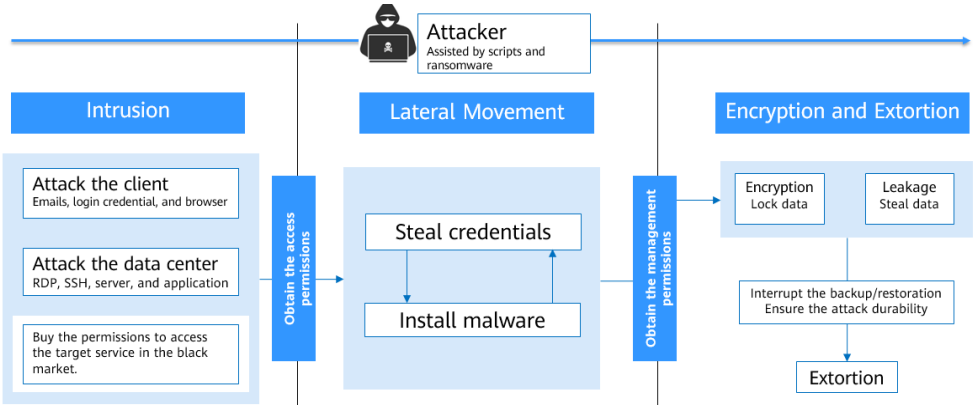
Scenario

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 5-1 Extortion process



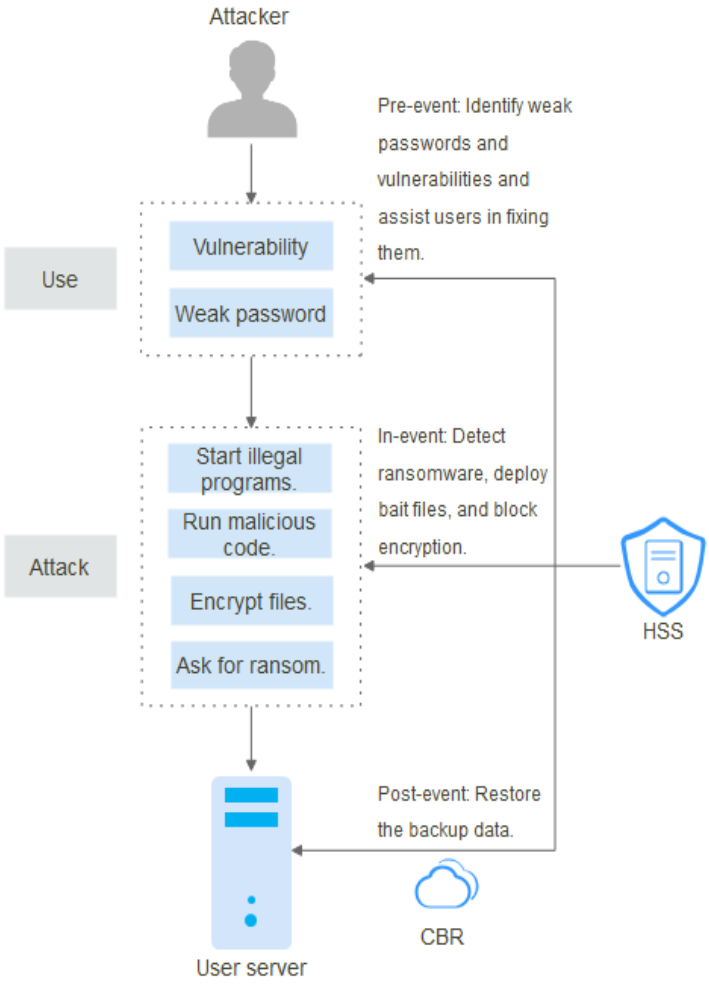
This solution describes how to use HSS and CBR to implement three-phase protection for servers, including pre-event prevention, in-event detection and timely blocking, and post-event backup and restoration.

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 5-2 HSS+CBR ransomware protection



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.

5.2 Resources and Costs

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

Table 5-1 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**.

5.3 Defense Measures

5.3.1 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.

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.

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.

       2) Fix vulnerabilities on the current server.

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

       NOTE

       - Use method 1 if you are fixing a vulnerability for the first time and cannot estimate impact on services. In this way, you can release the ECS at any time to save costs if the vulnerability fails to be fixed.
       - Use method 2 if you have fixed the vulnerability on similar servers before.

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

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

----End

5.3.2 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.

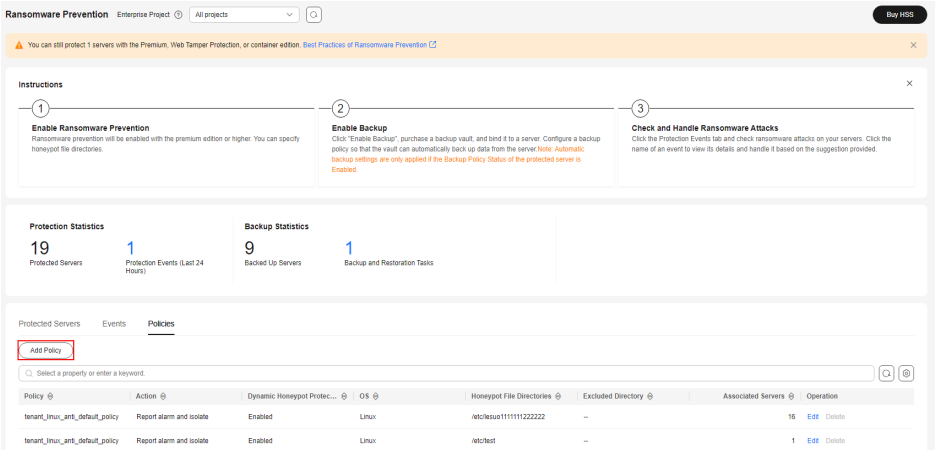
Step 1 Log in to the management console.

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 5-3 Adding a protection policy



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

Figure 5-4 Protection policy parameters

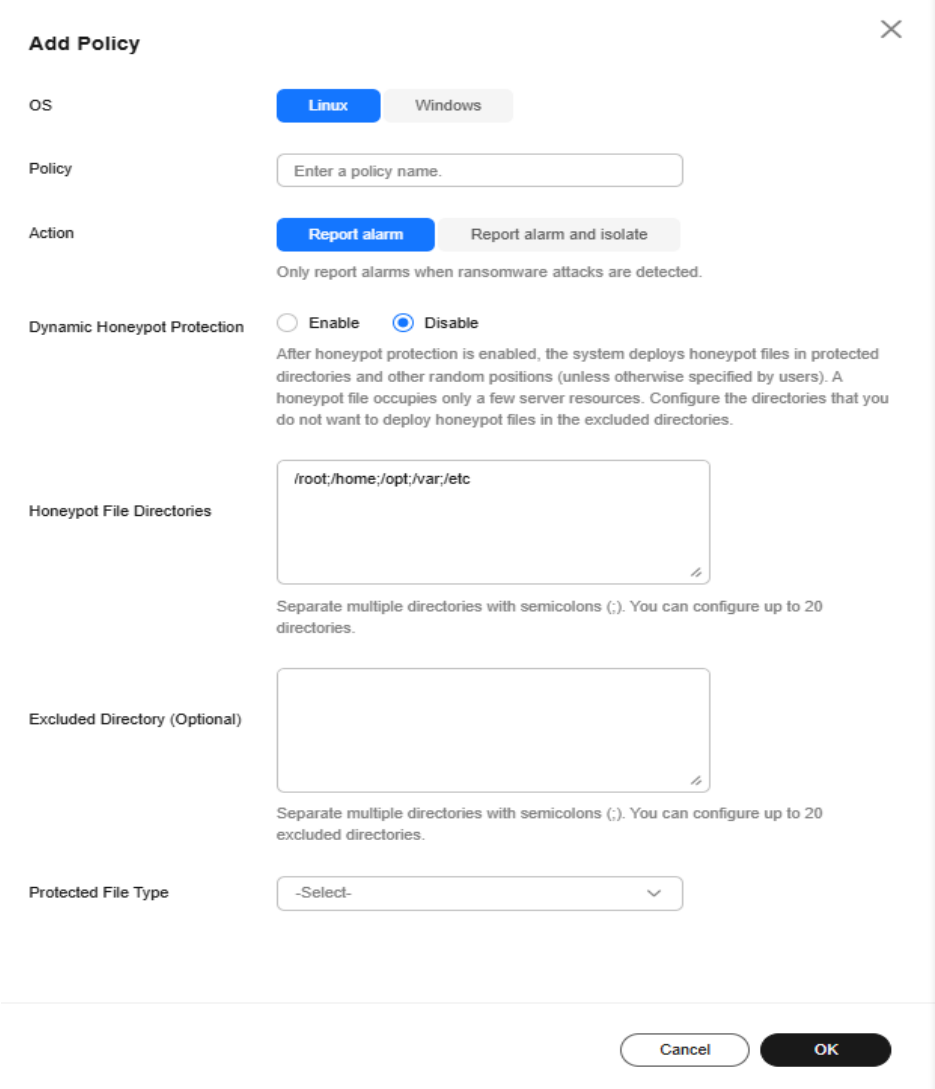


Table 5-2 Protection policy parameters

Parameter	Description	Example Value
OS	Server OS.	Linux
Policy	Policy name	test
Action	Indicates how an event is handled. • **Report alarm and isolate** • **Report alarm**	**Report alarm and isolate**

Parameter	Description	Example Value
Dynamic Honeypot Protection	After honeypot protection is enabled, the system deploys honeypot files in protected directories and other random 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. **NOTE** 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. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	Linux: **/etc** Windows: **C:\Test**
Excluded Directory (Optional)	Directory that does not need to be protected by honeypot files. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	Linux: **/etc/lesuo** Windows: **C:\Test\ProData**
File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. This parameter is mandatory for Linux servers only.	Select all

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. 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 and then enable the backup function.

Step 1 Log in to the management console.

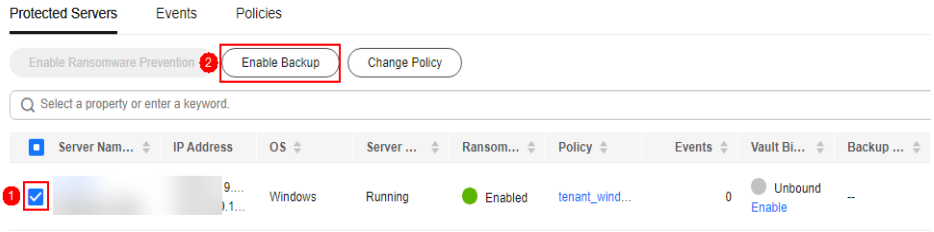
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **HSS**.

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 5-5 Enabling backup



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

NOTE

A vault that meets the following conditions can be bound:

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

Step 7 Click **OK**.

----End

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**.

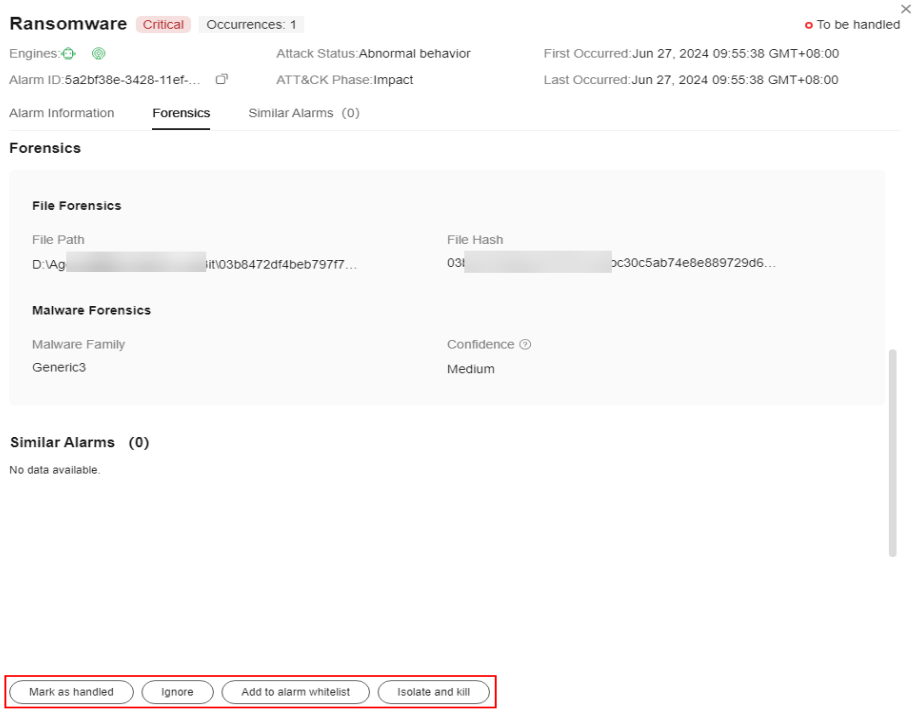
Step 4 Click the **Events** tab to view ransomware alarms.

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 5-6 Selecting an alarm handling mode



- **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.

5.3.3 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**.

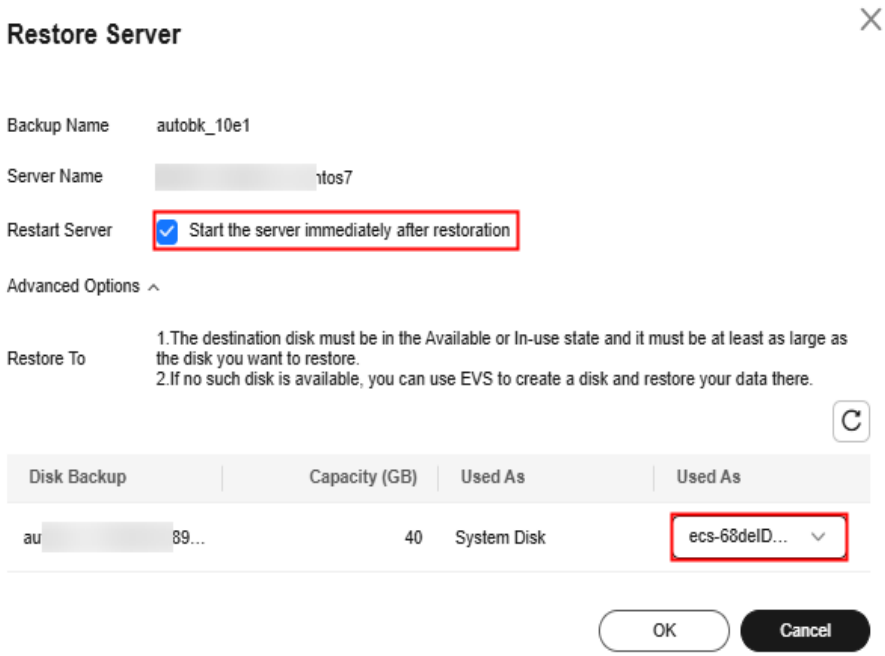
Step 6 In the displayed **Backups** page, select the backup data you want to restore.

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 5-7 Restoring a server



Step 9 Click **OK**.

----End

Related Operations

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

