Host Security Service

Getting Started

Issue	01
Date	2024-12-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Free Trial of HSS Basic Edition for 30 Days

When purchasing ECS, you can choose to use the HSS basic edition for free for 30 days. When the protection period expires, HSS is automatically disabled and no extra fee is charged. During the trial period, HSS can scan ECSs for security vulnerabilities and weak passwords and detect brute-force attacks. You can also log in to the HSS console to quickly view the security scores of your cloud assets, helping you learn about the security status and risks of your ECSs in a timely manner. For details about the protection functions during the free trial, see **Product Functions**.

How Can I Try Out Free HSS Basic Edition for 30 Days?

When purchasing an ECS, select **Basic edition (one-month free trial)** on **Configure Basic Settings** page. Then you can enjoy a 30-day free trial of HSS basic edition. For details about the supported OSs, see **Supported OSs**.

This section uses the following configuration as an example to describe how to use the HSS basic edition for free for 30 days.

- Quantity: 1
- Billing mode: yearly/Monthly
- Specifications: c6.xlarge.2 (2 vCPUs and 4GiB of memory)
- OS: Linux

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

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

Table 1-1 Parameter description

Parameter	Example	Description
Billing Mode	**Yearly/Monthly**	Prepaid billing. You pay in advance for a subscription term, and in exchange, you get a discounted rate. Ensure that you have a top-up account with a sufficient balance or have a valid payment method configured first. For more information, see **Pricing Details**.
Region	**EU-Dublin**	For lower network latency and quick resource access, select the region nearest to you. After an ECS is purchased, the region cannot be changed. Exercise caution when selecting a region.
AZ	**Random**	The system selects a default AZ based on your Universally Unique Identifier (UUID). The AZ of a purchased ECS cannot be changed.
CPU Architecture	**x86**	ECS provides multiple types of instance specifications of the x86 and Kunpeng architectures.
Instance	**c6.xlarge.2**	Select appropriate specifications based on service requirements. For more information, see the **ECS Specifications**.
Image	Select **Public image** and **Huawei Cloud EulerOS 2.0 Standard 64-bit (40 GiB)**.	A free public Linux image provided by Huawei Cloud.
Host protection (HSS)	**Select Host protection (HSS) and select Basic Edition.**	HSS Basic Edition is free for one month. It provides functions such as weak password and vulnerability detection.
Other parameters	-	Set this parameter based on project requirements. For details about parameter settings, see **Purchasing and Using a Linux ECS**.

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.

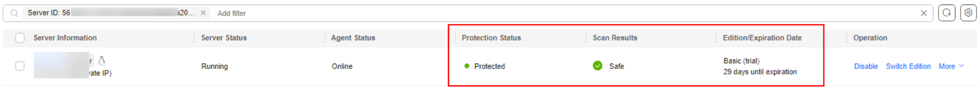
After the ECS is in the **Running** state, the HSS agent is automatically installed and the basic edition is enabled. This process takes about 20 minutes.

Step 4 Move the cursor to the **Security** column of the ECS and click **Learn more**. The HSS console page is displayed.

Step 5 The protection status of the cloud server is **Protected**, the edition is **Basic**, and the expiration time is **29 days until expiration**.

The trial period is successful. HSS provides basic security protection for your ECSs for 30 days.

Figure 1-1 Free trial of HSS basic edition for 30 days



Server ID: 56[redacted]20... × Add filter

□ Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Operation
□ [redacted] r ate IP)	Running	Online	● Protected	✓ Safe	Basic (trial) 29 days until expiration	Disable Switch Edition More

----End

What Should I Do When the Free Trial of HSS Basic Edition Expires?

When the 30-day free trial of HSS basic edition expires, HSS stops providing security protection for your servers. Its expiration has no impact on your servers. To continue using HSS, you can purchase and enable HSS after the free trial period expires. The procedure is as follows:

1. **Purchasing an HSS Quota**

   Purchase HSS editions based on your protection requirements. For details about the protection functions supported by each HSS edition, see Functions.

2. **Installing an Agent**

   During the free trial of HSS, the agent has been installed on the ECS by default. If you have uninstalled the agent, you need to reinstall it. If you have not uninstalled the agent, skip this step.

3. **Enabling Protection**

   HSS can be enabled only after this operation is performed.

2 Purchasing and Enabling HSS

Scenario

HSS helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions. There are also proactive protection and security operations functions available to help you easily detect and handle threats. For details about the server security protection functions provided by HSS, see **Product Functions**.

The following is an example to describe how to buy and enable HSS.

- Server: EulerOS 2.9 Huawei Cloud ECS
- Protection quotas
  - Billing mode: Yearly/Monthly
  - Version specification: Premium edition
  - Quantity: 1

Process

Procedure	Description
Preparations	After registering a Huawei Cloud and enabling Huawei Cloud services, complete real-name authentication, top up your account, grant permissions to IAM users, and prepare cloud servers to be protected.
Step 1: Purchase HSS Quota	Set the billing mode and edition, and purchase protection quota for your server.
Step 2: Install an Agent	Install the agent on the target server.
Step 3: Enable Protection	Enable protection for the target server.

Preparations

1. Before purchasing HSS, create a Huawei account and subscribe to Huawei Cloud. For details, see **Registering a Huawei ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

   If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Ensure that your account has sufficient funds to prevent failures in purchasing HSS protection quotas. For details, see **Topping Up an Account**.
3. If you perform operations as an IAM user, ensure that the IAM user has been assigned the **HSS FullAccess** permission. For details, see **Creating a User and Granting Permissions**.

   When purchasing HSS protection quotas, you need to assign the **BSS Administrator** permission to IAM users.
4. A Huawei Cloud ECS for which HSS will be enabled is available.

Step 1: Purchase HSS Quota

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 upper right corner of the Dashboard page, click **Buy HSS**.

Step 5 Configure parameters.

Table 2-1 Parameters for purchasing HSS

Parameter	Example	Description
Billing Mode	**Yearly/Monthly**	Select the billing mode. For more information, see **Pricing Details**. ● Yearly/Monthly: You can buy a prepaid yearly/monthly package if you intend to use the service for a long time. The fee is lower than that of pay-per-use. ● Pay-per-use: You pay for the used resources based on the actual service duration (in hours), without a minimum fee.
Region	**EU-Dublin**	Select the region of server. After the HSS is purchased, the region cannot be changed. Exercise caution when selecting a region.

Parameter	Example	Description
Edition Specifications	**Premium edition**	HSS provides basic, professional, premium, WTP, and container editions. Functions vary depending on editions. For details about functions supported by each edition, see **Functions**.
Enterprise Project	**default**	This parameter is displayed only when you use an enterprise account to purchase protection quotas. It enables unified management of cloud resources by project.
Tag	**Not added**	Tags are used to identify server security, facilitating cloud resource classification and management.
Automatically assign	**Not selected**	When a server or container node is added and the agent is installed for the first time, it will be bound to an available yearly/monthly quota. Only unused quotas will be bound, and **no new order or fee will be generated**.
Required Duration	**1 month**	Select the required duration. The longer the subscription period, the higher the discount. You do not need to configure the pay-per-use billing mode.
Auto-Renewal	**Not selected**	If this option is selected, the system automatically renews the service based on the subscription period. You do not need to configure the pay-per-use billing mode.
Quantity	**1**	Set the value based on the actual number of servers.

Step 6 In the lower right corner of the page, click **Next**.

Step 7 After confirming that the order, select **I have read and agree to the Host Security Service Disclaimer**.

Step 8 Click **Pay Now** and complete the payment.

Step 9 Click **Host Security Service** to return to the HSS console.

----End

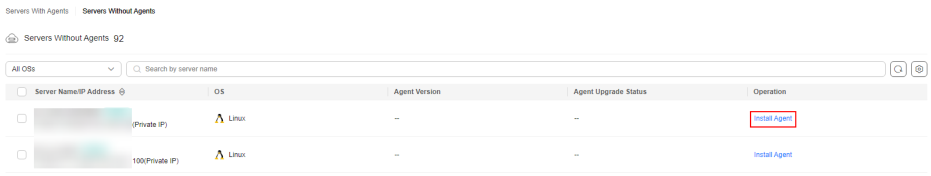
Step 2: Install an Agent

Step 1 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 2 Choose **Agents** > **Servers Without Agents**.

Step 3 In the **Operation** column of the target server, click **Install Agent**. The **Install Agent** dialog box is displayed.

Figure 2-1 Installing an agent



Servers With Agents | Servers Without Agents

Servers Without Agents 92

All OSs | Search by server name

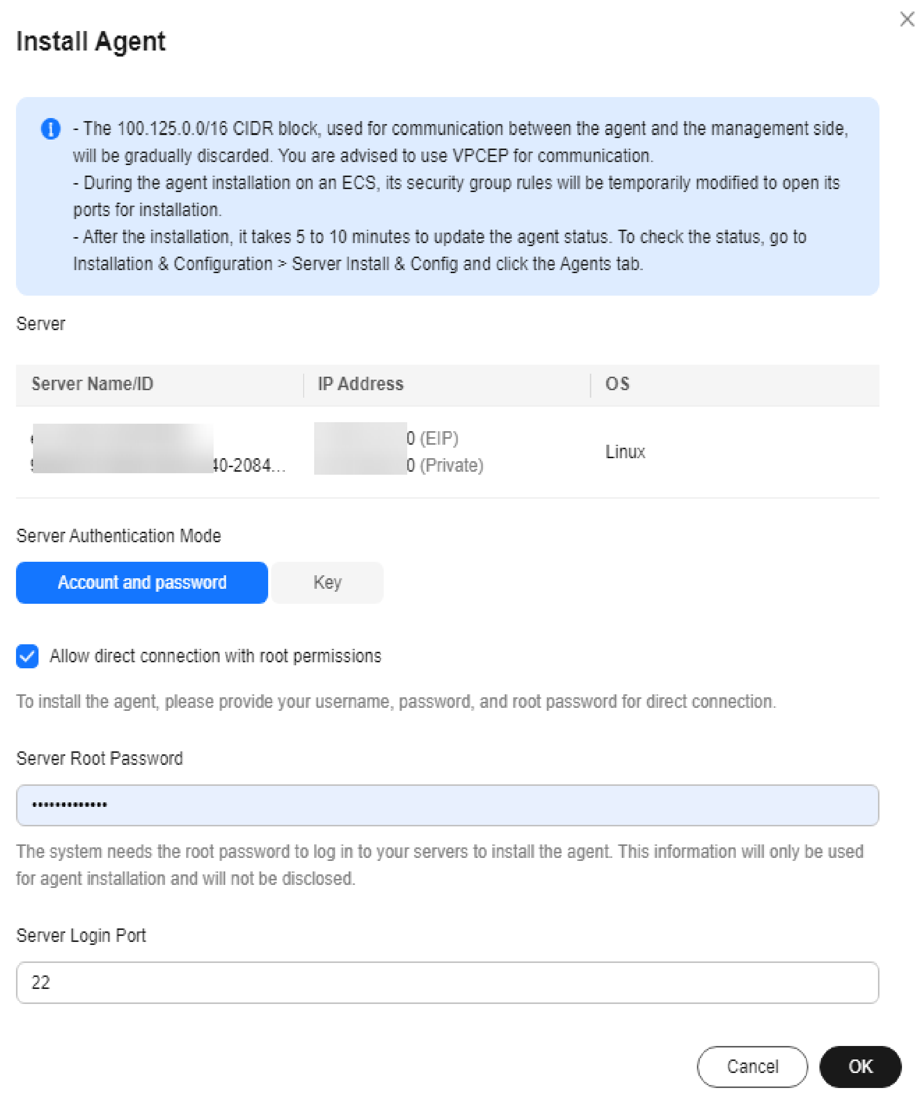
☐ Server Name/IP Address	OS	Agent Version	Agent Upgrade Status	Operation
☐ [redacted] (Private IP)	Linux	--	--	Install Agent
☐ [redacted] 100(Private IP)	Linux	--	--	Install Agent

Step 4 Select and set the server verification information.

Table 2-2 Parameters for installing the agent

Parameter	Example	Description
Server Authentication Mode	**Account and Password**	- Account and password: Use the server IP address and password to verify the installation. - Key: Authenticate the installation using a cloud key (in DEW) or a user-created key (Linux only).
Allow direct connection with root permissions	Select it.	The **root** account can be used to directly log in to the server. After you enter the **root** user password and login port, HSS will use your **root** account to install the agent for the server.
Server Root Password	-	Set the parameters based on the actual server information.
Server Login Port	**22**	Enter the actual login port of the server.

Figure 2-2 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]40-2084...	[redacted]0 (EIP) 0 (Private)	Linux

Server Authentication Mode

☑ 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 5 Click **OK** to start installation.

Step 6 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

Step 3: Enable Protection

Step 1 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

Step 2 In the **Operation** column of a server, click **Enable**.

Step 3 In the dialog box that is displayed, select the mode.

Table 2-3 Parameters for enabling protection

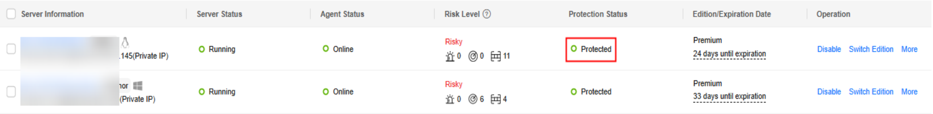
Parameter	Example	Description
Billing Mode	**Yearly/Monthly**	The value must be the same as the charging mode specified by **Step 1: Purchase HSS Quota**.
Edition	**Premium edition**	The value must be the same as the version selected in **Step 1: Purchase HSS Quota**.
Select Quota	**90e0ca09-ed16-4de0-b91c-ac7169beada9**	Select the quota purchased in **Step 1: Purchase HSS Quota**.

Step 4 After confirming the information, select **I have read and agree to the Host Security Service Disclaimer**.

Step 5 Click **OK**.

Step 6 If the **Protection Status** of the target server is **Protected**, the protection is enabled successfully.

Figure 2-3 Viewing the protection status



□ Server Information	Server Status	Agent Status	Risk Level ⓘ	Protection Status	Edition/Expiration Date	Operation
□ [redacted] .145(Private IP)	○ Running	○ Online	Risky 0 0 11	○ Protected	Premium 24 days until expiration	Disable Switch Edition More
□ [redacted] nor (Private IP)	○ Running	○ Online	Risky 0 6 4	○ Protected	Premium 33 days until expiration	Disable Switch Edition More

----End

Follow-Up Procedure

Enable active protection for servers.

HSS premium edition provides some proactive functions for servers. These functions are not enabled or not completely enabled when HSS is enabled. You can determine whether to use these functions based on your requirements, the following table **Table 2-4** describes the functions.

Table 2-4 Proactive server protection functions

Function	Description
Ransomware Prevention	Ransomware is one of the biggest cybersecurity threats today. Ransomware can intrude a server, encrypt data, and ask for ransom, causing service interruption, data leakage, or data loss. Attackers may not unlock the data even after receiving the ransom. HSS provides static and dynamic ransomware prevention. You can periodically back up server data to reduce potential losses. Ransomware prevention is automatically enabled with the WTP edition. Deploy bait files on servers and automatically isolate suspicious encryption processes. You can modify the ransomware protection policy.
Application Protection	To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.
Application Process Control	HSS can learn the characteristics of application processes on servers and manage their running. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes.
Virus scanning and removal	The function uses the virus detection engine to scan virus files on the server. The scanned file types include executable files, compressed files, script files, documents, images, and audio and video files. You can perform quick scan and full-disk scan on the server as required. You can also customize scan tasks and handle detected virus files in a timely manner to enhance the virus defense capability of the service system.
Dynamic Port Honeypot	The dynamic port honeypot function is a deception trap. It uses a real port as a bait port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect your resources.

3 Purchasing and Enabling WTP

Scenario

HSS provides static and dynamic (Tomcat) Web Tamper Protection (WTP) functions. WTP monitors website directories in real time, backs up files, and restores tampered files. In addition, multiple server security protection functions are provided. For details, see **Product Functions**.

The following is an example to describe how to and enable HSS.

- Server: EulerOS 2.9 Huawei Cloud ECS
- Protection quotas
  - Billing mode: Yearly/Monthly
  - Edition: WTP
  - Quantity: 1

Process

Procedure	Description
Preparations	After registering a Huawei Cloud and enabling Huawei Cloud services, complete real-name authentication, top up your account, grant permissions to IAM users, and prepare cloud servers to be protected.
Step 1: Purchase HSS Quota	Set the edition, and protection quota for your server.
Step 2: Install an Agent	Install the agent on the target server.
Step 3: Enable Protection	Enable protection for the target server.

Preparations

1. Before purchasing WTP, create a Huawei account and subscribe to Huawei Cloud. For details, see **Registering a Huawei ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

   If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Ensure that your account has sufficient funds to prevent failures in purchasing HSS protection quotas. For details, see **Topping Up an Account**.
3. If you perform operations as an IAM user, ensure that the IAM user has been assigned the **HSS FullAccess** permission. For details, see **Creating a User and Granting Permissions**.

   When purchasing HSS protection quotas, you need to assign the **BSS Administrator** permission to IAM users.
4. A Huawei Cloud ECS for which WTP will be enabled is available.

Step 1: Purchase HSS Quota

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 upper right corner of the Dashboard page, click **Buy HSS**.

Step 5 Configure parameters.

Parameter	Example	Description
Billing Mode	**Yearly/Monthly**	WTP supports only the **Yearly/ Monthly** billing mode. **Yearly/Monthly** is a prepaid billing. You pay in advance for a subscription term, and in exchange, you get a discounted rate. The longer the subscription term, the bigger the discount. For more information, see **Pricing Details**.
Region	**EU-Dublin**	Select the region of server. After the HSS is purchased, the region cannot be changed. Exercise caution when selecting a region.

Parameter	Example	Description
Edition Specifications	**WTP Edition**	HSS provides basic, professional, premium, WTP, and container editions. Functions vary depending on editions. For details about functions supported by each edition, see **Functions**.
Enterprise Project	**default**	This parameter is displayed only when you use an enterprise account to purchase protection quotas. It enables unified management of cloud resources by project.
Tag	**Not added**	Tags are used to identify server security, facilitating cloud resource classification and management.
Automatically assign	**Not selected**	When a server or container node is added and the agent is installed for the first time, it will be bound to an available yearly/monthly quota. Only unused quotas will be bound, and **no new order or fee will be generated**.
Required Duration	**1 month**	Select the required duration. The longer the subscription period, the higher the discount.
Auto-Renewal	**Not selected**	The **Auto-renew** option enables the system to renew your service by the required duration when the service is about to expire.
Quantity	**1**	Set the value based on the actual number of servers.

Step 6 In the lower right corner of the page, click **Next**.

Step 7 After confirming that the order, select **I have read and agree to the Host Security Service Disclaimer**.

Step 8 Click **Pay Now** and complete the payment.

Step 9 Click **Back to Host Security Service Console** to return to the HSS console.

----End

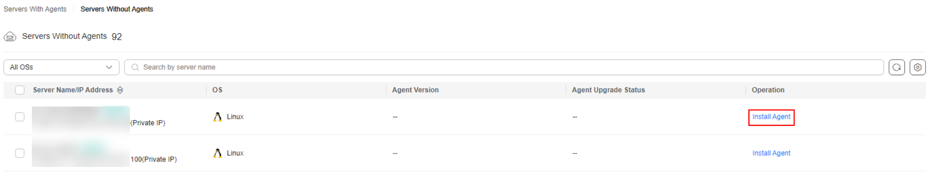
Step 2: Install an Agent

Step 1 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 2 Choose **Agents** > **Servers Without Agents**.

Step 3 In the **Operation** column of the target server, click **Install Agent**. The **Install Agent** dialog box is displayed.

Figure 3-1 Installing an agent



Servers With Agents | Servers Without Agents

Servers Without Agents 92

All OSs | Search by server name

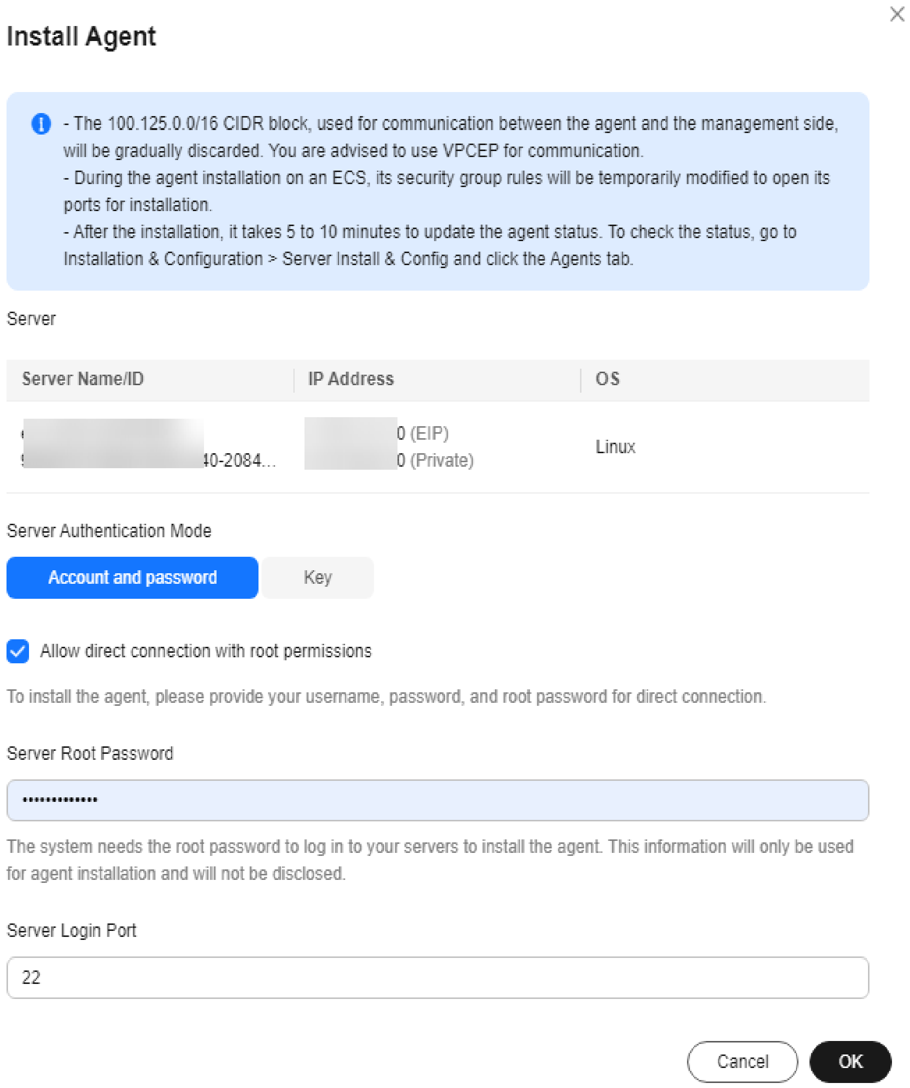
☐ Server Name/IP Address	OS	Agent Version	Agent Upgrade Status	Operation
☐ [redacted](Private IP)	Linux	--	--	Install Agent
☐ [redacted]100(Private IP)	Linux	--	--	Install Agent

Step 4 Select and set the server verification information.

Table 3-1 Parameters for installing the agent

Parameter	Example	Description
Server Authentication Mode	**Account and Password**	- Account and password: Use the server IP address and password to verify the installation. - Key: Authenticate the installation using a cloud key (in DEW) or a user-created key (Linux only).
Allow direct connection with root permissions	Select it.	The **root** account can be used to directly log in to the server. After you enter the **root** user password and login port, HSS will use your **root** account to install the agent for the server.
Server Root Password	**-**	Set the parameters based on the actual server information.
Server Login Port	**22**	Enter the actual login port of the server.

Figure 3-2 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]40-2084...	[redacted]0 (EIP) 0 (Private)	Linux

Server Authentication Mode

☑ 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 5 Click **OK** to start installation.

Step 6 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

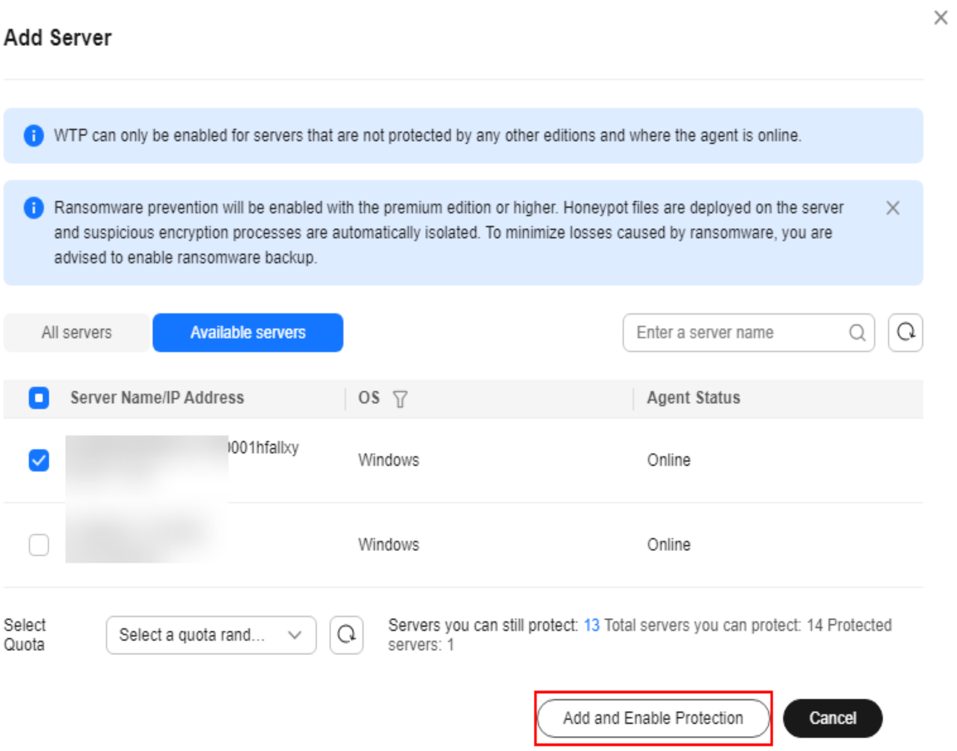
Step 3: Enable Protection

Step 1 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Step 2 On the **Servers** tab, click **Add Server**.

Step 3 On the **Add Server** page, select the target server and click **Add and Enable Protection**.

Figure 3-3 Adding a protected server



Add Server ×

WTP can only be enabled for servers that are not protected by any other editions and where the agent is online.

Ransomware prevention will be enabled with the premium edition or higher. Honeypot files are deployed on the server and suspicious encryption processes are automatically isolated. To minimize losses caused by ransomware, you are advised to enable ransomware backup.

All servers | **Available servers** | Enter a server name

■ Server Name/IP Address	OS	Agent Status
☑ [redacted])001hfallxy	Windows	Online
□ [redacted]	Windows	Online

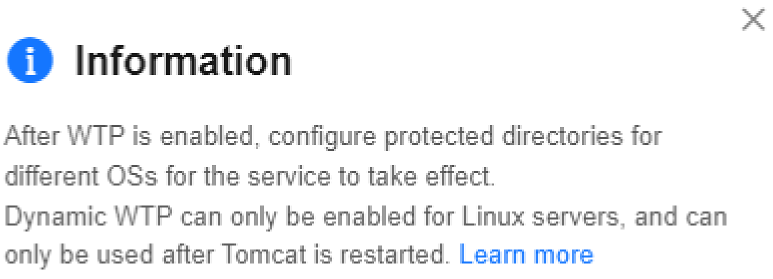
Select Quota: Select a quota rand...

Servers you can still protect: 13 Total servers you can protect: 14 Protected servers: 1

Add and Enable Protection | Cancel

Step 4 Read the message for adding a protected directory and click × .

Figure 3-4 Prompt information

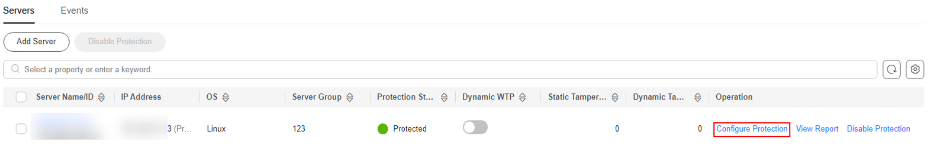


Information

After WTP is enabled, configure protected directories for different OSs for the service to take effect.
Dynamic WTP can only be enabled for Linux servers, and can only be used after Tomcat is restarted. Learn more

Step 5 Locate the row containing the target server and click **Configure Protection** in the **Operation** column.

Figure 3-5 Protection settings



Servers | Events

Add Server | Disable Protection

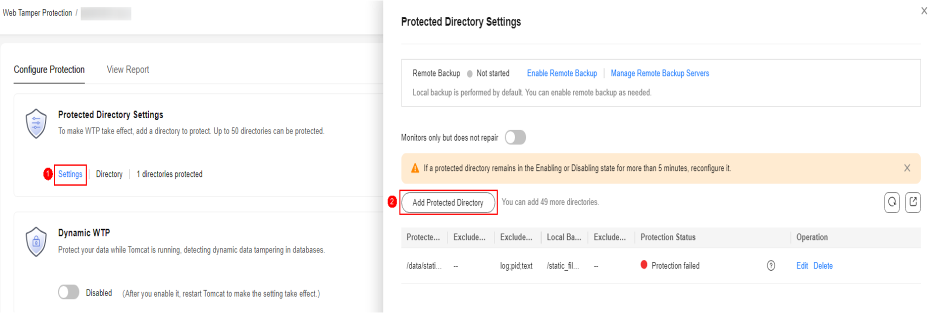
Select a property or enter a keyword.

□ Server Name/ID	IP Address	OS	Server Group	Protection St...	Dynamic WTP	Static Tamper...	Dynamic Ta...	Operation
□ [redacted]	[redacted]3 (Pr...	Linux	123	● Protected	○	0	0	Configure Protection View Report Disable Protection

Step 6 Add a protected directory.

1. In the **Protected Directory Settings** area, click **Settings**.
2. In the **Protected Directory Settings** dialog box, click **Add Protected Directory**.

Figure 3-6 Adding a protected directory



Web Tamper Protection / [redacted]

Configure Protection | View Report

Protected Directory Settings
To make WTP take effect, add a directory to protect. Up to 50 directories can be protected.

1 Settings | Directory | 1 directories protected

Dynamic WTP
Protect your data while Tomcat is running, detecting dynamic data tampering in databases.

Disabled (After you enable it, restart Tomcat to make the setting take effect.)

Protected Directory Settings

Remote Backup ● Not started Enable Remote Backup | Manage Remote Backup Servers
Local backup is performed by default. You can enable remote backup as needed.

Monitors only but does not repair

If a protected directory remains in the Enabling or Disabling state for more than 5 minutes, reconfigure it.

2 Add Protected Directory You can add 49 more directories.

Protecte...	Exclude...	Exclude...	Local Ba...	Exclude...	Protection Status	Operation
/data/stati...	--	log;pid;text	/static_fil...	--	● Protection failed	Edit Delete

3. Configure protected directories.

Table 3-2 Parameters for adding a protected directory

Parameter	Example	Description
Protected Directory	**/etc/lesuo**	Add directories to be protected. – Do not add an OS directory as a protected directory. – After a directory is added, the files and folders in the protected directory are read-only and cannot be modified directly.
Excluded Subdirectory	**lesuo/test**	Subdirectories that do not need to be protected in the protected directory, such as temporary file directories. Separate subdirectories with semicolons (;). A maximum of 10 subdirectories can be added.
Excluded File Types	**log;pid;text**	Types of files that do not need to be protected in the protected directory, such as log files. To record the running status of the server in real time, exclude the log files in the protected directory. You can grant high read and write permissions for log files to prevent attackers from viewing or tampering with the log files. Separate file types with semicolons (;).

Parameter	Example	Description
Local Backup Path	**/etc/backup**	Set this parameter if your server runs the Linux OS. Set a local backup path for files in protected directories. After WTP is enabled, files in the protected directory are automatically backed up to the local backup path. The backup rules are described as follows: – The local backup path must be valid and cannot overlap with the protected directory path. – Excluded subdirectories and types of files are not backed up. – Generally, the backup completes within 10 minutes. The actual duration depends on the size of files in the protected directory. – If WTP detects that a file in a protected directory is tampered with, it immediately uses the backup file on the local server to restore the file.
Excluded File Path	**lesuo/data;lesuo/list**	Exclude files that do not need to be protected from the protected directory. Separate multiple paths with semicolons (;). A maximum of 50 paths can be added. The maximum length of a path is 256 characters. A single path cannot start with a space or end with a slash (/).

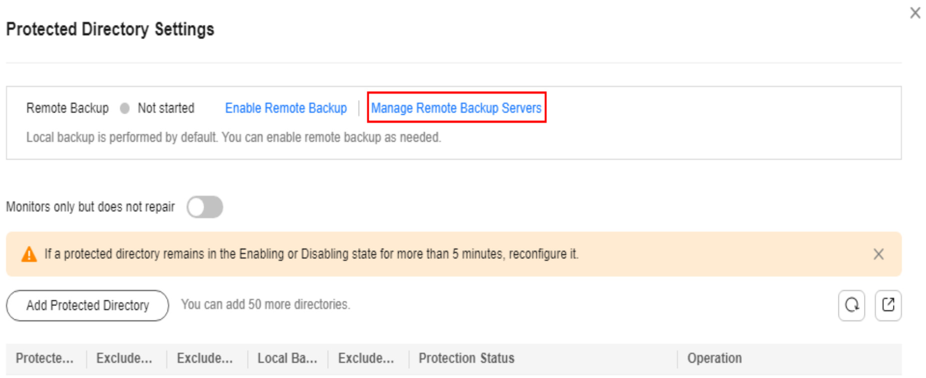
4. Click **OK**.
5. In the protected directory list, if **Protection Status** is **Protected**, the directory is added successfully.

Step 7 (Optional) Enable remote backup.

Only Linux servers support the remote backup function. Skip this item for Windows servers.

1. In the **Protected Directory Settings** dialog box, click **Manage Remote Backup Servers**.

Figure 3-7 Managing remote backup servers



Protected Directory Settings

Remote Backup ● Not started Enable Remote Backup | Manage Remote Backup Servers

Local backup is performed by default. You can enable remote backup as needed.

Monitors only but does not repair

If a protected directory remains in the Enabling or Disabling state for more than 5 minutes, reconfigure it.

Add Protected Directory You can add 50 more directories.

Protecte...	Exclude...	Exclude...	Local Ba...	Exclude...	Protection Status	Operation

2. Click **Add Backup Server**.
3. Configure the remote backup server information and click **OK**.

Table 3-3 Backup server parameters

Parameter	Example	Description
Server Name	**test**	Name of the remote backup server.
Address	**192.168.1.1**	Enter the private IP address of the Huawei Cloud as the remote backup server.
Port	**8080**	Enter the server port number. Ensure that the port is not blocked by any security group or firewall or occupied.

Parameter	Example	Description
Backup Path	**/hss01**	Enter a backup path. The content of the protected directory will be backed up to this path. – If the protected directories of multiple servers are backed up to the same remote backup server, the data will be stored in separate folders named after agent IDs. Assume the protected directories of the two servers are **/hss01** and **hss02**, and the agent IDs of the two servers are **f1fdbabc-6cdc-43af-acab-e4e6f086625f** and **f2ddbabc-6cdc-43af-abcd-e4e6f086626f**, and the remote backup path is **/hss01**. The corresponding backup paths are **/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f** and **/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f**. – If WTP is enabled for the remote backup server, do not set the remote backup path to any directories protected by WTP. Otherwise, remote backup will fail.

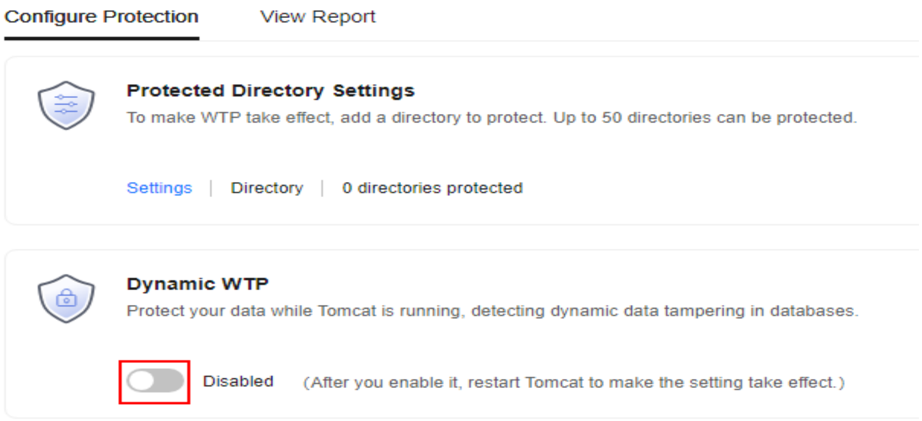
4. In the **Protected Directory Settings** area, click **Settings**.
5. In the **Protected Directory Settings** dialog box, click **Enable Remote Backup**.
6. Select the added remote backup server and click **OK**.
7. If **Enabled** is displayed, remote backup is started.

Step 8 (Optional) Enable dynamic WTP.

Runtime application self-protection (RASP) is provided for Tomcat applications of JDK 8 on a Linux server. If you do not require RASP of the Tomcat application or the server runs the Windows OS, skip this item.

1. In the **Dynamic WTP** area, click .

Figure 3-8 Enable dynamic WTP



Configure Protection | View Report

Protected Directory Settings

To make WTP take effect, add a directory to protect. Up to 50 directories can be protected.

Settings | Directory | 0 directories protected

Dynamic WTP

Protect your data while Tomcat is running, detecting dynamic data tampering in databases.

Disabled (After you enable it, restart Tomcat to make the setting take effect.)

2. In the dialog box that is displayed, enter the Tomcat bin directory and click **OK**.

   Tomcat bin directory example: **/usr/workspace/apache-tomcat-8.5.15/bin**

3. If is displayed, dynamic WTP is enabled.
4. Restart Tomcat to make the dynamic WTP function take effect.

----End

Follow-Up Procedure

- **Modify a file or folder in a protected directory.**

  If WTP is enabled, files or folders in the protected directory are read-only and cannot be modified. To modify files or folders in the protected directory, perform the following steps:

  - Adding a privileged process: A maximum of 10 privileged processes can be added. For details, see **Adding a Privileged Process**.
  - Enabling/Disabling scheduled static WTP: In addition to adding a privileged process, you can set periodic static WTP and modify files or folders when WTP is disabled, for details, see **Enabling/Disabling Scheduled Static WTP**.

- **Enable active protection for servers.**

  WTP provides some proactive functions for servers. These functions are not enabled or not completely enabled when WTP is enabled. You can determine whether to use these functions based on your requirements, the following table **Table 3-4** describes the functions.

Table 3-4 Proactive server protection functions

Function	Description
Ransomware Prevention	Ransomware is one of the biggest cybersecurity threats today. Ransomware can intrude a server, encrypt data, and ask for ransom, causing service interruption, data leakage, or data loss. Attackers may not unlock the data even after receiving the ransom. HSS provides static and dynamic ransomware prevention. You can periodically back up server data to reduce potential losses. Ransomware prevention is automatically enabled with the WTP edition. Deploy bait files on servers and automatically isolate suspicious encryption processes. You can modify the ransomware protection policy.
Application Protection	To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.
Application Process Control	HSS can learn the characteristics of application processes on servers and manage their running. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes.
Virus scanning and removal	The function uses the virus detection engine to scan virus files on the server. The scanned file types include executable files, compressed files, script files, documents, images, and audio and video files. You can perform quick scan and full-disk scan on the server as required. You can also customize scan tasks and handle detected virus files in a timely manner to enhance the virus defense capability of the service system.
Dynamic Port Honeypot	The dynamic port honeypot function is a deception trap. It uses a real port as a bait port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect your resources.

4 Purchasing and Enabling Container Security Protection

Scenario

A container cluster consists of a set of nodes. The HSS container edition uses nodes as protection units and provides functions such as container firewall, container cluster protection, and container image security scanning, helping enterprises solve container environment problems that cannot be achieved by traditional security software. For details about the server security protection functions provided by HSS container edition, see **Product Functions**.

The following is an example to describe how to buy and enable container protection.

- Container node: EulerOS 2.9 Huawei Cloud ECS
- Protection quotas
  - Billing mode: Yearly/Monthly
  - Edition: container
  - Quantity: 1

Process

Procedure	Description
Preparations	After registering a Huawei Cloud and enabling Huawei Cloud services, complete real-name authentication, top up your account, grant permissions to IAM users, and prepare container node resources to be protected.
Step 1: Purchase HSS Quota	Set the billing mode and edition, and purchase protection quota for the target container nodes.
Step 2: Install an Agent	Install the agent on the target container node.

Procedure	Description
Step 3: Enable Protection	Enable protection for the target container node.

Preparations

1. Before purchasing container protection, create a Huawei account and subscribe to Huawei Cloud. For details, see **Registering a Huawei ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

   If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.

2. Ensure that your account has sufficient funds to prevent failures in purchasing HSS protection quotas. For details, see **Topping Up an Account**.

3. If you perform operations as an IAM user, ensure that the IAM user has been assigned the **HSS FullAccess** permission. For details, see **Creating a User and Granting Permissions**.

   When purchasing HSS protection quotas, you need to assign the **BSS Administrator** permission to IAM users.

4. You have prepared a container node for which container security protection will be enabled.

Step 1: Purchase HSS Quota

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 upper right corner of the Dashboard page, click **Buy HSS**.

Step 5 Configure parameters.

Table 4-1 Parameters for purchasing HSS

Parameter	Example	Description
Billing Mode	**Yearly/Monthly**	Select the billing mode. For more information, see **Pricing Details**. ● Yearly/Monthly: You can buy a prepaid yearly/monthly package if you intend to use the service for a long time. The fee is lower than that of pay-per-use. ● Pay-per-use: You pay for the used resources based on the actual service duration (in hours), without a minimum fee.
Region	**EU-Dublin**	Select the region of container node. After the HSS is purchased, the region cannot be changed. Exercise caution when selecting a region.
Edition Specifications	**Container edition**	HSS provides basic, professional, premium, WTP, and container editions. Functions vary depending on editions. For details about functions supported by each edition, see **Functions**.
Enterprise Project	**default**	This parameter is displayed only when you use an enterprise account to purchase protection quotas. It enables unified management of cloud resources by project.
Tag	**Not added**	Tags are used to identify container security, facilitating cloud resource classification and management.
Automatically assign	**Not selected**	When a server or container node is added and the agent is installed for the first time, it will be bound to an available yearly/monthly quota. Only unused quotas will be bound, and **no new order or fee will be generated**.
Required Duration	**1 month**	Select the required duration. The longer the subscription period, the higher the discount. You do not need to configure the pay-per-use billing mode.

Parameter	Example	Description
Auto-Renewal	**Not selected**	If this option is selected, the system automatically renews the service based on the subscription period. You do not need to configure the pay-per-use billing mode.
Quantity	**1**	Set the value based on the actual number of container nodes.

Step 6 In the lower right corner of the page, click **Next**.

Step 7 After confirming that the order, select **I have read and agree to the Host Security Service Disclaimer**.

Step 8 Click **Pay Now** and complete the payment.

Step 9 Click **Host Security Service** to return to the HSS console.

----End

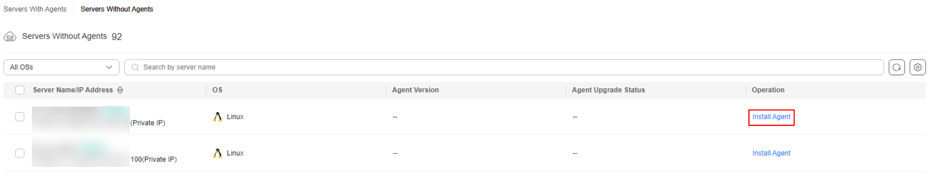
Step 2: Install an Agent

Step 1 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 2 Choose **Agents** > **Servers Without Agents**.

Step 3 In the **Operation** column of the target server, click **Install Agent**. The **Install Agent** dialog box is displayed.

Figure 4-1 Installing an agent



Servers With Agents | Servers Without Agents

Servers Without Agents 92

All OSs | Search by server name

Server Name/IP Address	OS	Agent Version	Agent Upgrade Status	Operation
[redacted] (Private IP)	Linux	--	--	Install Agent
[redacted] 100(Private IP)	Linux	--	--	Install Agent

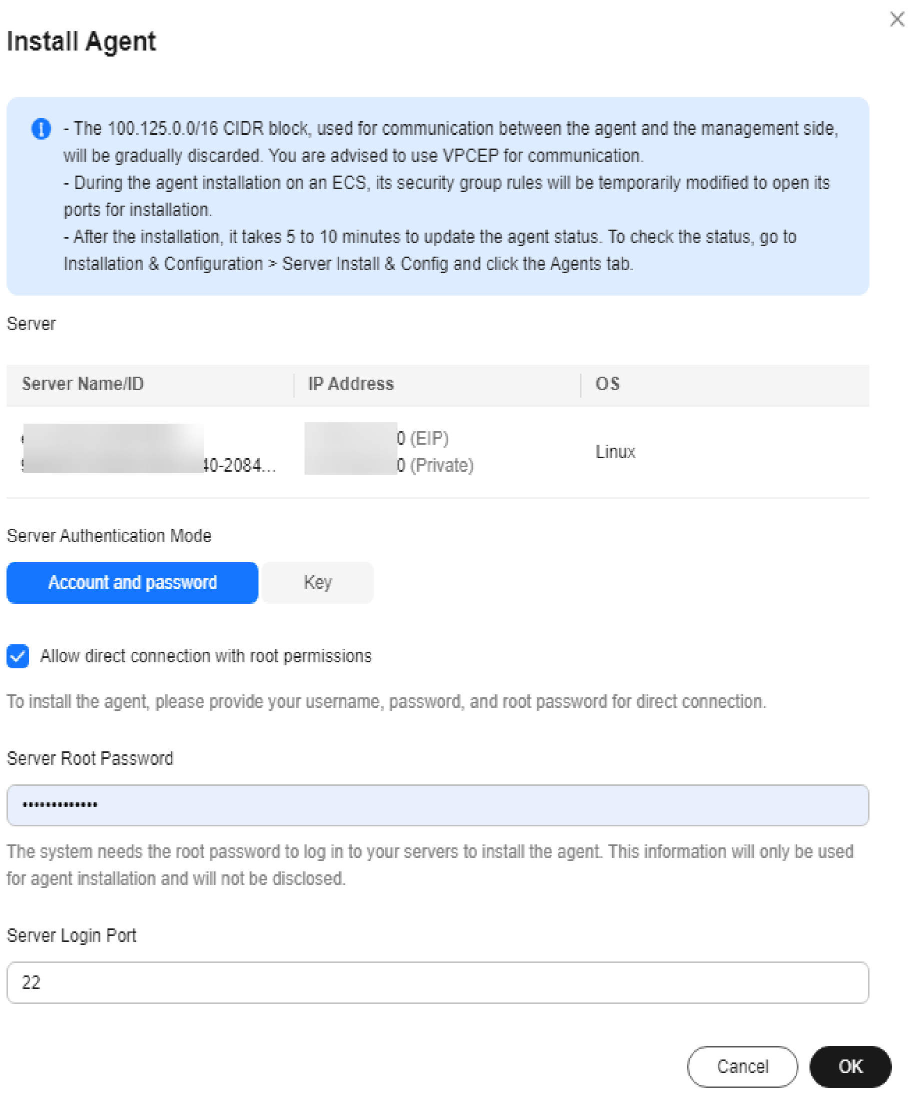
Step 4 Select and set the server verification information.

Table 4-2 Parameters for installing the agent

Parameter	Example	Description
Server Authentication Mode	**Account and Password**	● Account and password: Use the server IP address and password to verify the installation. ● Key: Authenticate the installation using a cloud key (in DEW) or a user-created key (Linux only).

Parameter	Example	Description
Allow direct connection with root permissions	Select it.	The **root** account can be used to directly log in to the server. After you enter the **root** user password and login port, HSS will use your **root** account to install the agent for the server.
Server Root Password	**-**	Set the parameters based on the actual server information.
Server Login Port	**22**	Enter the actual login port of the server.

Figure 4-2 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]40-2084...	[redacted]0 (EIP) 0 (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 5 Click **OK** to start installation.

Step 6 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

Step 3: Enable Protection

Step 1 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 2 In the **Operation** column of a server, click **Enable**.

Step 3 In the dialog box that is displayed, select the mode.

Table 4-3 Parameters for enabling protection

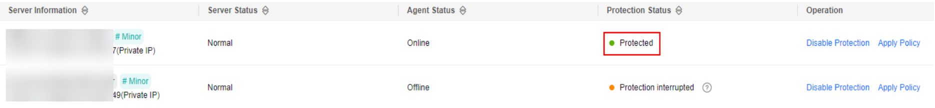
Parameter	Example	Description
Billing Mode	**Yearly/Monthly**	The value must be the same as the charging mode specified by **Step 1: Purchase Protection Quota**.
Edition	**Container edition**	The value must be the same as the edition specified by **Step 1: Purchase Protection Quota**.
Select Quota	**709440b9-0d6c-407e-a51c-ac7169beada9**	Select the quota purchased in **Step 1: Purchase Protection Quota**.

Step 4 Confirm the information, read the *Container Security Service Disclaimer*, and select **I have read and agree to the Container Security Service Disclaimer**.

Step 5 Click **OK**.

Step 6 If the **Protection Status** of the target server is **Protected**, the protection is enabled successfully.

Figure 4-3 Viewing the protection status



Server Information	Server Status	Agent Status	Protection Status	Operation

[redacted] # Minor
7(Private IP)
	Normal	Online	● Protected	Disable Protection Apply Policy

[redacted] # Minor
49(Private IP)
	Normal	Offline	● Protection interrupted	Disable Protection Apply Policy

----End

Follow-Up Procedure

Enable server protection for container nodes.

HSS container edition provides some proactive functions for servers. These functions are not enabled or not completely enabled when container security protection is enabled. You can determine whether to use these functions based on your requirements, the following table **Table 4-4** describes the functions.

Table 4-4 Container node protection functions

Function	Description
Container Image Security Scanning	The container image security scanning function scans for vulnerabilities and malicious files in images. You are advised to scan images periodically so that you can handle image security risks in a timely manner.

Function	Description
Ransomware Prevention	Ransomware is one of the biggest cybersecurity threats today. Ransomware can intrude a server, encrypt data, and ask for ransom, causing service interruption, data leakage, or data loss. Attackers may not unlock the data even after receiving the ransom. HSS provides static and dynamic ransomware prevention. You can periodically back up server data to reduce potential losses. Ransomware prevention is automatically enabled with the container edition. Deploy bait files on servers and automatically isolate suspicious encryption processes. You can modify the ransomware protection policy. You are also advised to enable backup so that you can restore data.
Application Protection	To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.
Application Process Control	HSS can learn the characteristics of application processes on servers and manage their running. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes.
Virus scanning and removal	The function uses the virus detection engine to scan virus files on the server. The scanned file types include executable files, compressed files, script files, documents, images, and audio and video files. You can perform quick scan and full-disk scan on the server as required. You can also customize scan tasks and handle detected virus files in a timely manner to enhance the virus defense capability of the service system.
Container Firewall	A container firewall controls and intercepts network traffic inside and outside a container cluster to prevent malicious access and attacks.

5 Quickly Viewing ECS Security Situation

ECSs that are not protected by HSS are scanned for free in the early morning on each Monday. This section describes how to view the security situation of ECSs that are not protected by HSS.

If you use HSS to protect ECSs, you can refer to this section to quickly view the security situation of ECSs.

Viewing the Security Situation of ECSs That Are Not Protected

Step 1 Log in to the management console.

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

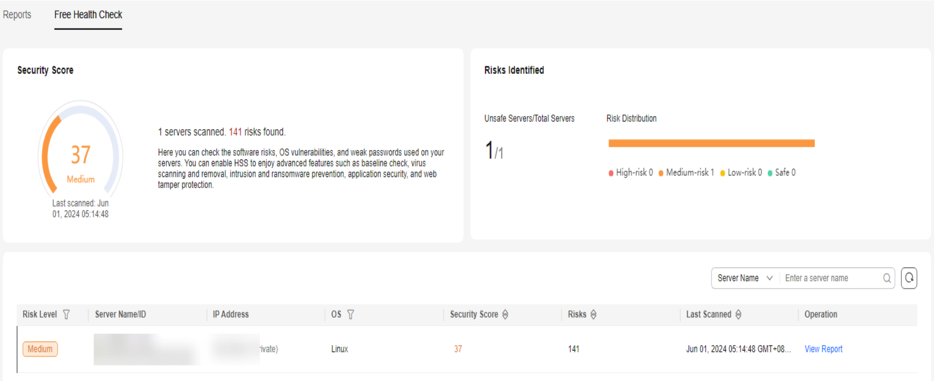
Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > HSS.

Step 4 In the navigation pane on the left, choose **Security Operations** > **Reports**.

Step 5 Select the **Free Health Check** tab.

Step 6 View the security situation of ECSs that are not protected.

Figure 5-1 View security situation


Reports
Free Health Check
Security Score
37
Medium
Last scanned: Jun 01, 2024 05:14:48
Risks Identified
Unsafe Servers/Total Servers
1/1
Risk Distribution
● High-risk 0 ● Medium-risk 1 ● Low-risk 0 ● Safe 0
Server Name
Enter a server name

1 servers scanned. 141 risks found.

Here you can check the software risks, OS vulnerabilities, and weak passwords used on your servers. You can enable HSS to enjoy advanced features such as baseline check, virus scanning and removal, intrusion and ransomware prevention, application security, and web tamper protection.

Risk Level	Server Name/ID	IP Address	OS	Security Score	Risks	Last Scanned	Operation
Medium	[redacted]	[redacted]ivate)	Linux	37	141	Jun 01, 2024 05:14:48 GMT+08...	View Report

- Security Score: displays the security scores of all ECSs in the current region and the risks.

- Risks Identified: displays the percentage of risky servers and the risk level distribution.
- Report: To view the detailed health check report of an ECS, click **View Report** in the **Operation** column of a target ECS.

  NOTE

  – A free health check report is generated on the first day of each month. You can only view the report online but cannot download it.

  – In the report, up to five results can be displayed for each check item. If a check item has fewer than five results, only half of them will be displayed.

----End

Viewing the Security Situation of ECSs for Which Protection Has Been Enabled

Step 1 Log in to the management console.

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

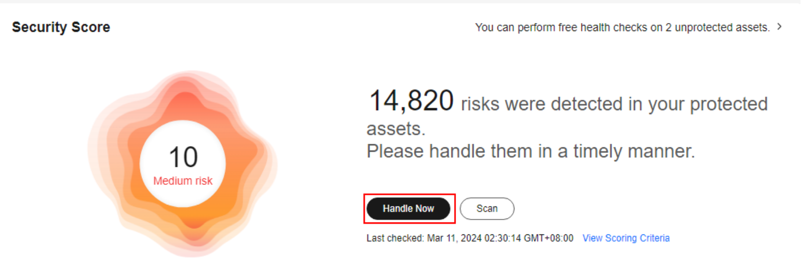
Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > HSS.

Step 4 View the ECS security situation.

- **View the security situation of all ECSs.**
  - Viewing the security score
    1. In the **Security Score** area on the **Dashboard** page, view the security risk scores of all your ECSs. Click **Handle Now** to view risks of your assets.

       For details about scoring criteria and how to improve your score, see **Security Score Deduction**.

       Figure 5-2 Viewing the security score

       Security Score

       You can perform free health checks on 2 unprotected assets. >

       14,820 risks were detected in your protected assets.
       Please handle them in a timely manner.

       Last checked: Mar 11, 2024 02:30:14 GMT+08:00 View Scoring Criteria

    2. In the **Handle Now** dialog box, click ⌄ to view risk details.
    3. Click **Handle** to go to the risk details page and view and handle security risks.
  - View the security risk distribution and trend.
    1. In the **Security Risks** area on the **Dashboard** page, view the security risk distribution of the asset and the security risk trend in the last seven days.

ii. You can click the value of the server risks or container risks to go to the details page and view and handle the risk.

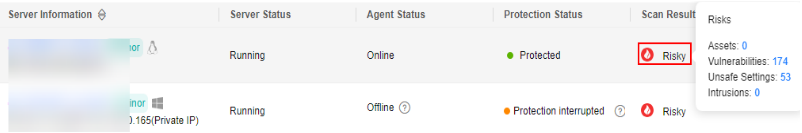
- **View the security situation of an ECS.**

  a. In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

  b. In the **Scan Results** column of the target server, check whether the ECS is risky.

  Move the cursor to the risky icon to view the risk distribution.

  Figure 5-3 Viewing ECS security situation



Server Information	Server Status	Agent Status	Protection Status	Scan Result
[redacted] ior	Running	Online	● Protected	Risky
[redacted] inor).165(Private IP)	Running	Offline ?	● Protection interrupted ?	Risky

Risks

Assets: 0
Vulnerabilities: 174
Unsafe Settings: 53
Intrusions: 0

  c. Click the ECS name to go to the ECS details page and view and handle security risks.

----End

6 Getting Started with Common Practices

After enabling protection, you can use a series of common practices provided by HSS to meet your service requirements.

Table 6-1 Common practices

Practice		Description
Server login protection	**Using HSS to Enhance Host Login Security**	HSS login protection greatly improves server security.
Vulnerability fixing	**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. This practice describes how to use HSS to detect and fix the vulnerability.
	SaltStack Remote Command Execution Vulnerabilities (CVE-2020-11651 and CVE-2020-11652)	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 servers, and obtain sensitive information. This practice describes how to use HSS to detect and fix the vulnerability.

Practice		Description
	OpenSSL High-risk Vulnerability (CVE-2020-1967)	OpenSSL security notice released update information regarding the 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. This practice describes how to use HSS to detect and fix the vulnerability.
	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. This practice describes how to use HSS to detect and fix the vulnerability.
	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. This practice describes how to use HSS to detect and fix the vulnerability.
	Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)	This vulnerability (CVE-2020-0601) 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. This practice describes how to use HSS to detect and fix the vulnerability.

Practice		Description
Ransomware prevention	**Using HSS and CBR to Defend Against Ransomware**	Ransomware attacks have become one of the biggest security challenges facing companies today. Attackers use ransomware encryption to lock the victim's data or asset devices and demand a payment to unlock the data. Sometimes, attackers may not unlock the data even after receiving the ransom. To prevent ransomware attacks and huge economic loss, you can use "HSS+CBR" to provide pre-event, in-event, and post-event ransomware protection for servers.