

Host Security Service

Getting Started

Issue 01
Date 2024-03-26



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei 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 Getting Started with Common Practices.....	1
2 Free Trial of HSS Basic Edition for 30 Days.....	4
3 Quickly Enabling HSS.....	6
4 Quickly Enabling WTP.....	11
5 Quickly Enabling Container Security Protection.....	21
6 ECS Security Situation Quick Reference.....	26

1 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 1-1 Common practices

Practice		Description
Server login protection	Best Practices of Login Security Hardening	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
<p>OpenSSL High-risk Vulnerability (CVE-2020-1967)</p>	<p>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.</p> <p>This practice describes how to use HSS to detect and fix the vulnerability.</p>
<p>Adobe Font Manager Library Remote Code Execution Vulnerability (CVE-2020-1020/CVE-2020-0938)</p>	<p>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.</p> <p>This practice describes how to use HSS to detect and fix the vulnerability.</p>
<p>Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027)</p>	<p>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.</p> <p>This practice describes how to use HSS to detect and fix the vulnerability.</p>
<p>Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)</p>	<p>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.</p> <p>This practice describes how to use HSS to detect and fix the vulnerability.</p>

Practice		Description
Multi-cloud server management	HSS multi-cloud management	To monitor workloads and centrally manage resources of the clouds and on hybrid clouds, HSS provides a security solution that helps you manage Huawei Cloud and hybrid clouds in a unified manner. HSS allows you to use the same security policies on different clouds, preventing the risks caused by inconsistent security policies.
Ransomware prevention	Best Practices for Defense 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.
Web tamper protection	Combining WAF and HSS to Get Improved Web Tamper Protection	With HSS and WAF in place, you can stop worrying about web page tampering.

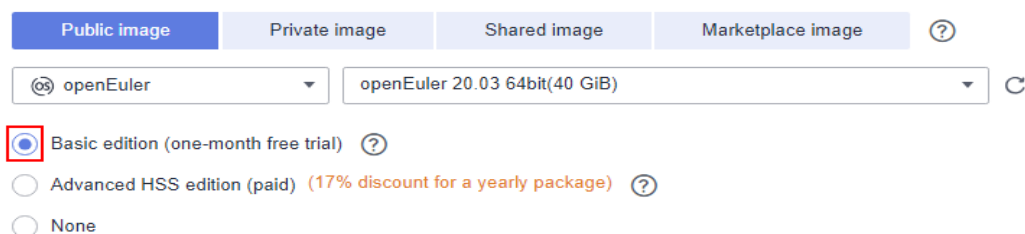
2 Free Trial of HSS Basic Edition for 30 Days

When purchasing ECS, you can choose to use the basic edition for free for 30 days. For details about the supported protection functions, see [Specifications of Different Editions](#).

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](#).

Figure 2-1 Select free trial



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. **Purchase quota**

Purchase HSS editions based on your protection requirements. For details about the supported protection functions, see [Specifications of Different Editions](#).

2. **Installing the 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. **Enable Protection**

HSS can be enabled only after this operation is performed.

3 Quickly 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 protection functions of server security, see [Specifications of Different Editions](#).

This document uses an ECS running EulerOS 2.9 as an example to describe how to quickly enable HSS.

Prerequisites

- The ECS is in the **Running** state and can access the Internet.
- Ensure the outbound rule of your security group allows access to the port 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- The DNS server address of the cloud server has been set to the private DNS server address. For details, see [Changing the DNS Server Address of an ECS](#) and [Private DNS Server Addresses](#).
- The available capacity of the disk where the agent is installed must be greater than 300 MB. Otherwise, the agent installation may fail.
- The Security-Enhanced Linux (SELinux) firewall has been disabled. The firewall affects agent installation and should remain disabled until the agent is installed.
- If any third-party security software has been installed on your server, the HSS agent may fail to be installed. In this case, disable or uninstall the software before installing the agent.

Constraints

- 64-bit Huawei Cloud servers and non-Huawei Cloud servers can be protected. 32-bit servers are no longer supported.
- Mainstream OSs are supported. For details, see [Supported OSs](#).
- The HSS agent will be automatically installed on Workspace 23.6.0 or later. If your Workspace version is earlier than 23.6.0, you can manually install the agent by referring to this section.

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 and choose **Security & Compliance > Host Security Service**. The HSS console is displayed.
- Step 4** In the upper right corner of the Dashboard page, click **Buy HSS**.
- Step 5** Set the parameters for buying HSS as prompted. For details, see [Table 3-1](#).

Table 3-1 Parameters for purchasing HSS

Parameter	Description
Billing Mode	Select Yearly/Monthly .
Region	Select the region of server.
Edition	Select Enterprise .
Enterprise Project	<p>This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects.</p> <ul style="list-style-type: none"> You can contact your service manager to enable this function You can select an enterprise project from the drop-down list. <p>NOTE</p> <ul style="list-style-type: none"> Resources and incurred expenses are managed under the enterprise project you selected. Value default indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project. The default option is available in the Enterprise Project drop-down list only after you purchased HSS under your Huawei ID.
Required Duration	<p>Select 1 month and select Auto-renew.</p> <p>If you select Auto-renew, the system will automatically renew your subscription as long as your account balance is sufficient. The renewal period is the same as the required duration.</p>
Server Quota	Set the Server Quota to 1.
Tag	<ul style="list-style-type: none"> If no predefined tag is available, click View predefined tags to create a predefined tag. If you have predefined tags, click the Tag key and Tag value boxes in sequence to select a predefined tag.

Parameter	Description
Quota Management	<p>Select Assigning automatically.</p> <p>After automatic quota binding is enabled, HSS automatically binds available quotas to new servers or container nodes after the agent is installed for the first time. Only the yearly/monthly quotas that you have purchased can be automatically bound. No new order or fee is generated.</p> <ul style="list-style-type: none"> • Servers: Available yearly/monthly quotas are automatically bound in the following sequence: Premium Edition > Enterprise Edition > Professional Edition > Basic Edition. • Container nodes: Available yearly/monthly quotas are automatically bound in the following sequence: Container Edition > Premium Edition > Enterprise Edition > Professional Edition > Basic Edition.

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

For details about pricing, see [Product Pricing Details](#).

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**.

----End

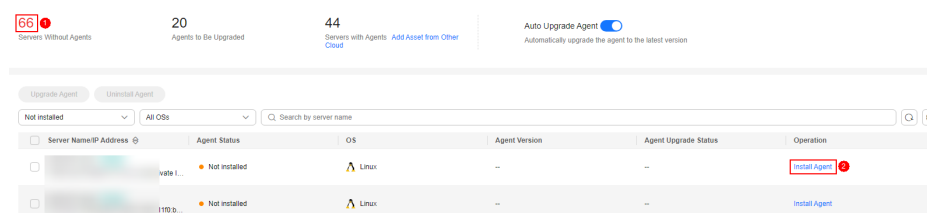
Step 2: Install an Agent

Step 1 Log in to the HSS console, in the navigation pane on the left, choose **Installation & Configuration**.

Step 2 On the agent management tab, Click the value of **Servers Without Agents** area to filter the servers that have not installed agents.

Step 3 In the **Operation** column of a server, click **Install Agent**.

Figure 3-1 Installing an agent



Step 4 In the dialog box, click **Copy** to copy the command for installing the agent.

Step 5 Remotely log in to the server where the agent is to be installed.

Step 6 Run the copied installation command as user **root** to install the agent on the server.

If the command output shown in **Installation completed** is displayed, the agent is successfully installed.

Figure 3-2 Installation completed

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

Step 7 Run the following command to check the runtime status of agent:

service hostguard status

If the command output shown in **Agent running properly** is displayed, the agent is running properly.

Figure 3-3 Agent running properly

```
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
```

----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 3-2** describes the parameters for enabling protection.

Table 3-2 Parameters for enabling protection

Parameter	Description
Billing Mode	Select Yearly/Monthly .
Edition	Select Enterprise .
Select Quota	Retain the default random 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 3-4 Viewing the protection status

Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Operation
	Running	Online	Protected	Risky	Web Tamper Protection	Disable Switch Edition More
 (Private IP)	Running	Offline	Protection interrupted	Risky	Premium (trial) 107 days until expiration	Disable Switch Edition More

----End

4 Quickly 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 [Specifications of Different Editions](#).

This document uses an ECS running EulerOS 2.9 as an example to describe how to quickly protect WTP.

Prerequisites

- The ECS is in the **Running** state and can access the Internet.
- Ensure the outbound rule of your security group allows access to the port 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- The DNS server address of the cloud server has been set to the private DNS server address. For details, see [Changing the DNS Server Address of an ECS](#) and [Private DNS Server Addresses](#).
- The available capacity of the disk where the agent is installed must be greater than 300 MB. Otherwise, the agent installation may fail.
- The Security-Enhanced Linux (SELinux) firewall has been disabled. The firewall affects agent installation and should remain disabled until the agent is installed.
- If any third-party security software has been installed on your server, the HSS agent may fail to be installed. In this case, disable or uninstall the software before installing the agent.

Constraints

- 64-bit Huawei Cloud servers and non-Huawei Cloud servers can be protected. 32-bit servers are no longer supported.
- Mainstream OSs are supported. For details, see [Supported OSs](#).
- The HSS agent will be automatically installed on Workspace 23.6.0 or later. If your Workspace version is earlier than 23.6.0, you can manually install the agent by referring to this section.

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 and choose **Security & Compliance > Host Security Service**. The HSS console is displayed.
- Step 4** In the upper right corner of the Dashboard page, click **Buy HSS**.
- Step 5** Set the parameters for buying HSS as prompted. For details, see [Table 4-1](#).

Table 4-1 Parameters for purchasing HSS

Parameter	Description
Billing Mode	Select Yearly/Monthly .
Region	Select the region of server.
Edition	Select Web Tamper Protection .
Enterprise Project	This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects. <ul style="list-style-type: none">You can contact your service manager to enable this functionYou can select an enterprise project from the drop-down list. NOTE <ul style="list-style-type: none">Resources and incurred expenses are managed under the enterprise project you selected.Value default indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project.The default option is available in the Enterprise Project drop-down list only after you purchased HSS under your Huawei ID.
Required Duration	Select 1 month and select Auto-renew . If you select Auto-renew , the system will automatically renew your subscription as long as your account balance is sufficient. The renewal period is the same as the required duration.
Server Quota	Set the Server Quota to 1.
Tag	<ul style="list-style-type: none">If no predefined tag is available, click View predefined tags to create a predefined tag.If you have predefined tags, click the Tag key and Tag value boxes in sequence to select a predefined tag.

Parameter	Description
Quota Management	<p>Select Assigning automatically.</p> <p>After automatic quota binding is enabled, HSS automatically binds available quotas to new servers or container nodes after the agent is installed for the first time. Only the yearly/monthly quotas that you have purchased can be automatically bound. No new order or fee is generated.</p> <ul style="list-style-type: none"> • Servers: Available yearly/monthly quotas are automatically bound in the following sequence: Premium Edition > Enterprise Edition > Professional Edition > Basic Edition. • Container nodes: Available yearly/monthly quotas are automatically bound in the following sequence: Container Edition > Premium Edition > Enterprise Edition > Professional Edition > Basic Edition.

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

For details about pricing, see [Product Pricing Details](#).

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**.

----End

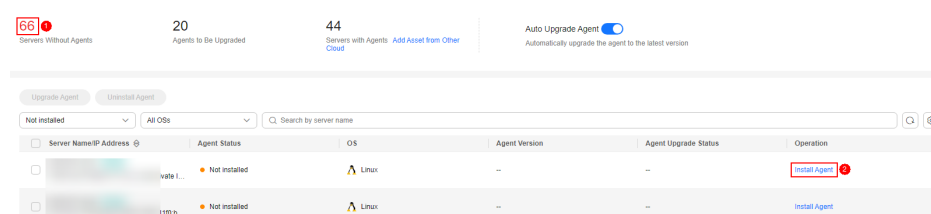
Step 2: Install an Agent

Step 1 Log in to the HSS console, in the navigation pane on the left, choose **Installation & Configuration**.

Step 2 On the agent management tab, Click the value of **Servers Without Agents** area to filter the servers that have not installed agents.

Step 3 In the **Operation** column of a server, click **Install Agent**.

Figure 4-1 Installing an agent



Step 4 In the dialog box, click **Copy** to copy the command for installing the agent.

Step 5 Remotely log in to the server where the agent is to be installed.

Step 6 Run the copied installation command as user **root** to install the agent on the server.

If the command output shown in **Installation completed** is displayed, the agent is successfully installed.

Figure 4-2 Installation completed

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

Step 7 Run the following command to check the runtime status of agent:

service hostguard status

If the command output shown in **Agent running properly** is displayed, the agent is running properly.

Figure 4-3 Agent running properly

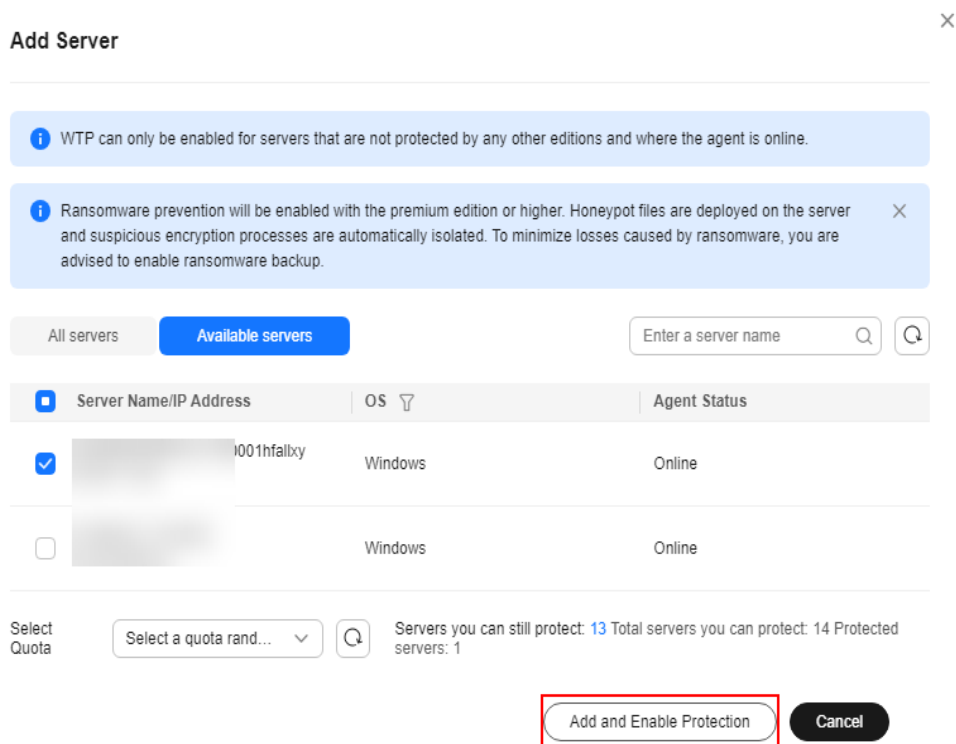
```
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
```


----End

Step 3: Enable Protection

- Step 1** In the navigation pane, choose **Prevention > 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 4-4 Adding a protected server



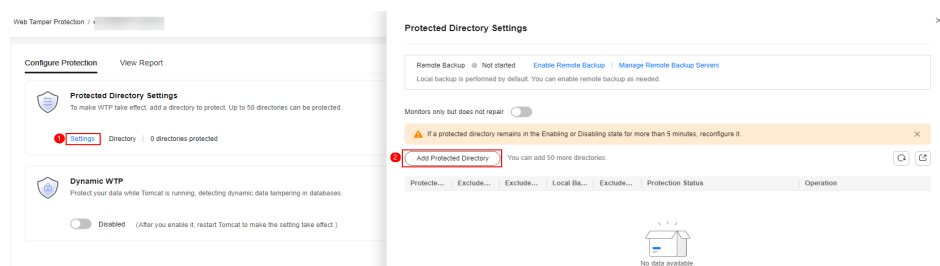
Step 4 Read the message for adding a protected directory and click .

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

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 4-5 Adding a protected directory



3. Add protected directories based on service requirements. For details about the parameters, see [Table 4-2](#).

Table 4-2 Parameters for adding a protected directory

Parameter	Description	Example Value
Protected Directory	<p>Add directories to be protected.</p> <ul style="list-style-type: none"> - 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. 	/etc/lesuo
Excluded Subdirectory	<p>Subdirectories that do not need to be protected in the protected directory, such as temporary file directories.</p> <p>Separate subdirectories with semicolons (;). A maximum of 10 subdirectories can be added.</p>	lesuo/test
Excluded File Types	<p>Types of files that do not need to be protected in the protected directory, such as log files.</p> <p>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.</p> <p>Separate file types with semicolons (;).</p>	log;pid;text

Parameter	Description	Example Value
Local Backup Path	<p>Set this parameter if your server runs the Linux OS.</p> <p>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.</p> <p>The backup rules are described as follows:</p> <ul style="list-style-type: none"> - 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. 	/etc/backup
Excluded File Path	<p>Exclude files that do not need to be protected from the protected directory.</p> <p>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 (/).</p>	lesuo/data;lesuo/list

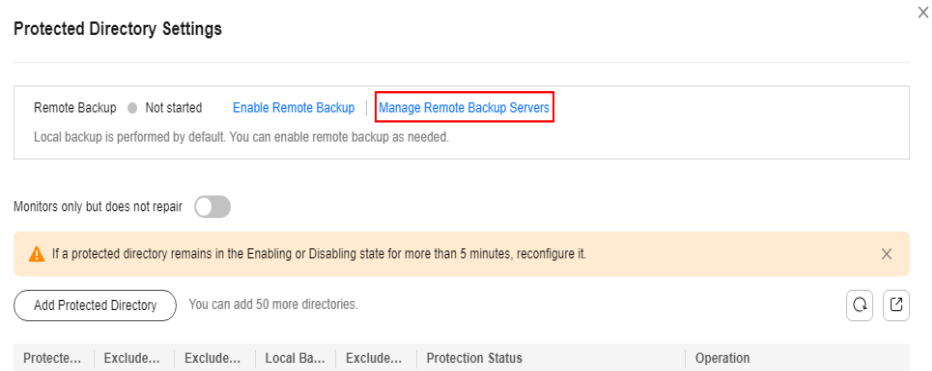
4. Click **OK**.
5. In the protected directory list, if **Protection Status** is **Protected**, the directory is added successfully.

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 4-6 Managing remote backup servers



2. Click **Add Backup Server**.
3. Enter the information and click **OK**. For details about the parameters, see [Table 4-3](#).

Table 4-3 Backup server parameters

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

Parameter	Description	Example Value
Backup Path	<p>Enter a backup path. The content of the protected directory will be backed up to this path.</p> <ul style="list-style-type: none"> - 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. 	/f1fdbabc-6cdc-43af-acab-e4e6f086625f

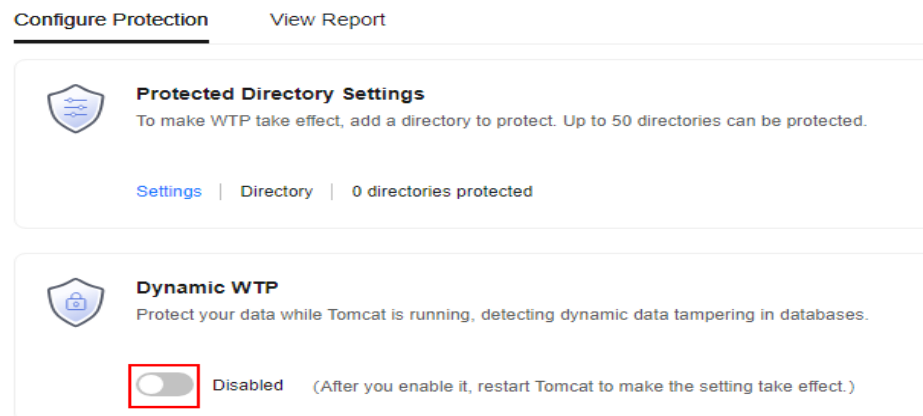
4. In the **Protected Directory Settings** area, click **Settings**.
5. In the **Protected Directory Settings** dialog box, click **Enable Remote Backup**.
6. Select the added remote backup server and click **OK**.
7. If **Enabled** is displayed, remote backup is started.

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 4-7 Enable dynamic WTP



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

3. If  is displayed, dynamic WTP is enabled.

----End

5 Quickly 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 security protection functions, see [Specifications of Different Editions](#).

This document uses a EulerOS 2.9 container node server as an example to describe how to quickly enable container security protection.

Prerequisites

- The ECS is in the **Running** state and can access the Internet.
- Ensure the outbound rule of your security group allows access to the port 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- The DNS server address of the cloud server has been set to the private DNS server address. For details, see [Changing the DNS Server Address of an ECS](#) and [Private DNS Server Addresses](#).
- The available capacity of the disk where the agent is installed must be greater than 300 MB. Otherwise, the agent installation may fail.
- The Security-Enhanced Linux (SELinux) firewall has been disabled. The firewall affects agent installation and should remain disabled until the agent is installed.
- If any third-party security software has been installed on your server, the HSS agent may fail to be installed. In this case, disable or uninstall the software before installing the agent.

Constraints

- 64-bit Huawei Cloud servers and non-Huawei Cloud servers can be protected. 32-bit servers are no longer supported.
- Mainstream OSs are supported. For details, see [Supported OSs](#).

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 and choose **Security & Compliance > Host Security Service**. The HSS console is displayed.
- Step 4** In the upper right corner of the Dashboard page, click **Buy HSS**.
- Step 5** Set the parameters for buying HSS as prompted. For details, see [Table 5-1](#).

Table 5-1 Parameters for purchasing HSS

Parameter	Description
Billing Mode	Select Yearly/Monthly .
Region	Select the region of container node.
Edition	Select Container .
Enterprise Project	<p>This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects.</p> <ul style="list-style-type: none"> You can contact your service manager to enable this function You can select an enterprise project from the drop-down list. <p>NOTE</p> <ul style="list-style-type: none"> Resources and incurred expenses are managed under the enterprise project you selected. Value default indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project. The default option is available in the Enterprise Project drop-down list only after you purchased HSS under your Huawei ID.
Required Duration	<p>Select 1 month and select Auto-renew.</p> <p>If you select Auto-renew, the system will automatically renew your subscription as long as your account balance is sufficient. The renewal period is the same as the required duration.</p>
Node Quantity	Set the Node Quantity to 1.
Tag	<ul style="list-style-type: none"> If no predefined tag is available, click View predefined tags to create a predefined tag. If you have predefined tags, click the Tag key and Tag value boxes in sequence to select a predefined tag.

Parameter	Description
Quota Management	<p>Select Assigning automatically.</p> <p>After automatic quota binding is enabled, HSS automatically binds available quotas to new servers or container nodes after the agent is installed for the first time. Only the yearly/monthly quotas that you have purchased can be automatically bound. No new order or fee is generated.</p> <ul style="list-style-type: none"> • Servers: Available yearly/monthly quotas are automatically bound in the following sequence: Premium Edition > Enterprise Edition > Professional Edition > Basic Edition. • Container nodes: Available yearly/monthly quotas are automatically bound in the following sequence: Container Edition > Premium Edition > Enterprise Edition > Professional Edition > Basic Edition.

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

For details about pricing, see [Product Pricing Details](#).

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**.

----End

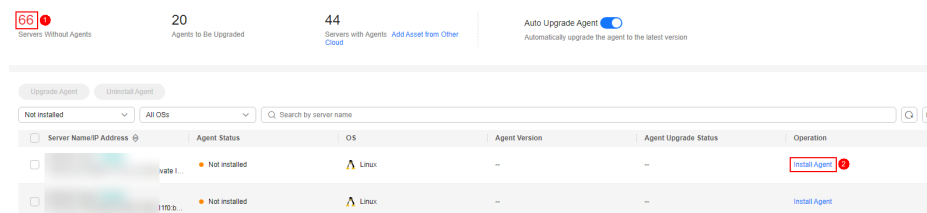
Step 2: Install an Agent

Step 1 Log in to the HSS console, in the navigation pane on the left, choose **Installation & Configuration**.

Step 2 On the agent management tab, Click the value of **Servers Without Agents** area to filter the servers that have not installed agents.

Step 3 In the **Operation** column of a server, click **Install Agent**.

Figure 5-1 Installing an agent



Step 4 In the dialog box, click **Copy** to copy the command for installing the agent.

Step 5 Remotely log in to the server where the agent is to be installed.

Step 6 Run the copied installation command as user **root** to install the agent on the server.

If the command output shown in **Installation completed** is displayed, the agent is successfully installed.

Figure 5-2 Installation completed

```

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

Step 7 Run the following command to check the runtime status of agent:

service hostguard status

If the command output shown in **Agent running properly** is displayed, the agent is running properly.

Figure 5-3 Agent running properly

```

your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
    
```

----End

Step 3: Enable Protection

- Step 1** In the navigation pane on the left, choose **Asset Management > Containers & Quota**.
- Step 2** In the **Operation** column of a server, click **Enable Protection**.
- Step 3** In the dialog box that is displayed, select the mode. **Table 5-2** describes the parameters for enabling protection.

Table 5-2 Parameters for enabling protection

Parameter	Description
Billing Mode	Select Yearly/Monthly .
Edition	Select Container .
Select Quota	Retain the default random 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 5-4 Viewing the protection status



Server Information	Server Status	Agent Status	Protection Status	Operation
# Minor 7 (Private IP)	Normal	Online	Protected	Disable Protection Apply Policy
# Minor 59 (Private IP)	Normal	Offline	Protection interrupted ⓘ	Disable Protection Apply Policy

----End

6 ECS Security Situation Quick Reference

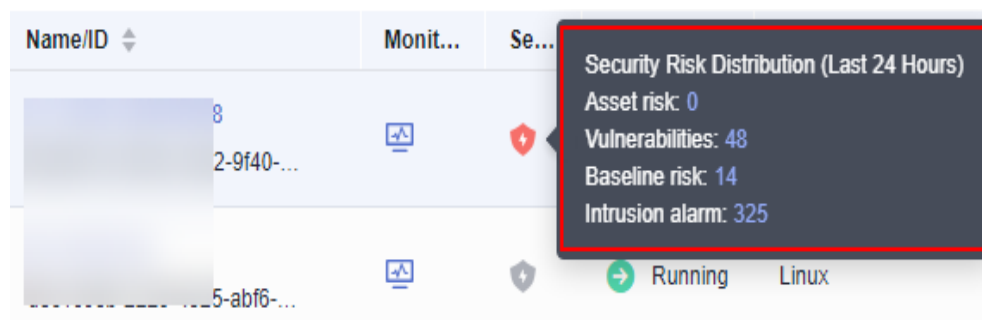
If you use HSS to protect ECSs, you can refer to this section to quickly view the security situation of ECSs.

Viewing ECS Security Situation on the ECS Console

- 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 and **Compute > Elastic Cloud Server**.
- Step 4** You can view the ECS security situation on the **Security** column of the target cloud server.


You can also view the number of asset risks, vulnerability risks, baseline risks, and intrusion alarm events in the last 24 hours. Click a risk value to go to the risk details list and view and handle security risks.


Figure 6-1 Viewing ECS security situation



----End

Viewing ECS Security Situation on the HSS Console

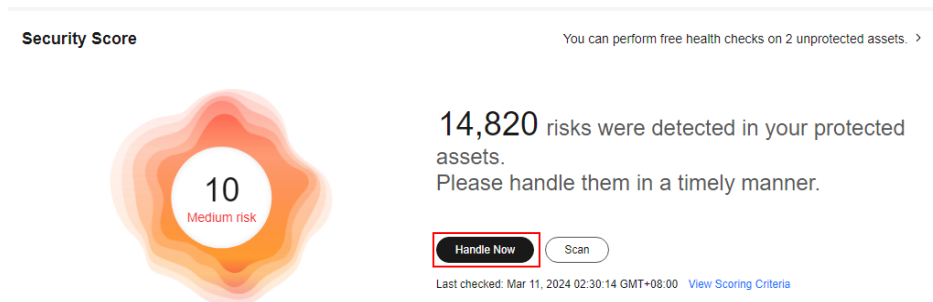
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select the region and project.

Step 3 Click  in the upper left corner and choose **Security & Compliance > Host Security Service**. The HSS console is displayed.

Step 4 View the ECS security situation.

- **View the security situation of all ECSs.**
 - a. 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 6-2 Viewing the security score




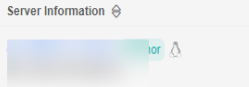



- b. In the **Handle Now** dialog box, click  to view risk details.
 - c. Click **Handle** to go to the risk details page and view and handle security risks.
- **View the security situation of an ECS.**
 - a. In the navigation pane on the left, choose **Asset Management > Servers & Quota**.
 - b. In 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 6-3 Viewing ECS security situation

Server Information	Server Status	Agent Status	Protection Status	Scan Result	Risks
	Running	Online	Protected		Assets: 0 Vulnerabilities: 174 Unsafe Settings: 53 Intrusions: 0
 .165(Private IP)	Running	Offline	Protection interrupted		

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

----End