

**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

---

<b>1 Free Trial of HSS Basic Edition for 30 Days.....</b>	<b>1</b>
<b>2 Purchasing and Enabling HSS.....</b>	<b>4</b>
<b>3 Purchasing and Enabling WTP.....</b>	<b>7</b>
<b>4 Purchasing and Enabling Container Security Protection.....</b>	<b>16</b>
<b>5 Quickly Viewing ECS Security Situation.....</b>	<b>21</b>
<b>6 Getting Started with Common Practices.....</b>	<b>24</b>

# 1 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](#).

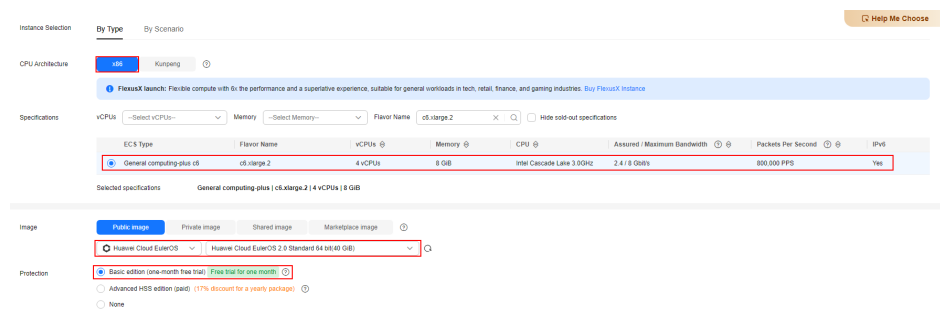
This document uses a yearly/monthly ECS (specifications: c6.xlarge.2; image: Huawei Cloud EulerOS 2.0 Standard 64 bit) as an example to describe how to use HSS basic edition for free for 30 days.

**Step 1** [Log in to the ECS console and buy an ECS](#).

**Step 2** On the **Buy ECS** page, set parameters related to **Configure Basic Settings**, **Configure Network**, **Configure Advanced Settings**, and **Confirm**.

1. Set basic configuration parameters and click **Next: Network Configuration**.
  - CPU Architecture: In this example, select **x86**.
  - Specifications: In this example, select **c6.xlarge.2**.
  - Image: In this example, select **Public image Huawei Cloud EulerOS 2.0 Standard 64 bit (40 GiB)**.
  - Protection: Select **Basic edition (one-month free trial) Free trial for one month**.
  - Configure other parameters based on site requirements.

**Figure 1-1 Basic settings**



2. Set network configuration parameters and click **Next: Configure Advanced Settings**.  
Set this parameter based on project requirements.
3. Set advanced parameters and click **Next: Confirm**.  
Set this parameter based on project requirements.
4. Set the parameters related to **confirm**.
  - Agreement: Read and agree to the *Image Disclaimer*.
  - Configure other parameters based on site requirements.

**Step 3** After confirming that all information is correct, click **Submit**. After the payment is complete, the ECS is automatically created and started by default.

After the ECS is in the **Running** status, 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 page is displayed.

**Step 5** The **Protection Status** of the ECS is **Protected**, the edition is **Basic Edition**, and the expiration time is **30 days until expiration**.

The trial use of the HSS basic edition is successful.

----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. **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.

# 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 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 purchase and enable HSS.

## 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.

- **Billing Mode:** Select a billing mode as required. In this example, select **Yearly/Monthly**.
- **Region:** Select the region where the server is located. In this example, select **CN-Hong Kong**.
- **Edition:** Select the HSS edition. Different editions provide different protection functions. In this example, select **Enterprise Edition**.
- **Quantity:** Set this parameter based on the number of servers. In this example, set the quantity to **1**.
- Specify other parameters as needed.

**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**.

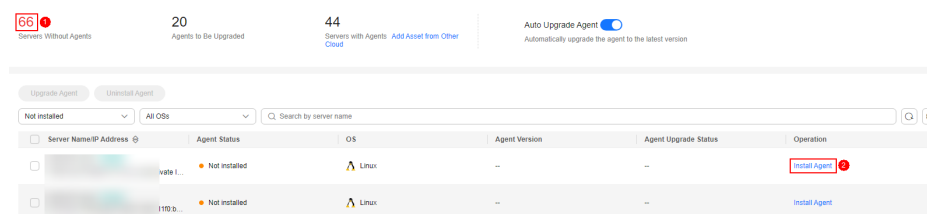
- Step 8** Click **Pay Now** and complete the payment.
- Step 9** Click **Back to Host Security Service Console**.

----End

## Step 2: Install an Agent

- Step 1** Log in to the HSS console, in the navigation pane on the left, choose **Installation & Configuration > Server Install & Config**.
- 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 2-1** 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 2-2** Installation completed



- 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 2-3 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.

Set this parameter based on the edition of the purchased quota in [Step 1: Purchase HSS Quota](#).

- **Billing Mode:** Select **Yearly/Monthly**.
- **Edition:** Select **Enterprise Edition**.

**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 2-4 Viewing the protection status

Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Operation
	Running	Online	<span style="border: 1px solid red; padding: 2px;">Protected</span>	<span style="color: red;">Risky</span>	Web Tamper Protection	<a href="#">Disable</a> <a href="#">Switch Edition</a> <a href="#">More</a>
 (Private IP)	Running	Offline	<span style="color: orange;">Protection interrupted</span>	<span style="color: red;">Risky</span>	Premium (trial) 107 days until expiration	<a href="#">Disable</a> <a href="#">Switch Edition</a> <a href="#">More</a>

----End

# 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 [Specifications of Different Editions](#).

This document uses an ECS running EulerOS 2.9 as an example to describe how to purchase and enable WTP.

## 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.

- Billing Mode: Select **Yearly/Monthly**. Only the **yearly/monthly** billing mode is supported.
- Region: Select the region where the server is located. In this example, select **CN-Hong Kong**.
- Edition: Select **Web Tamper Protection**.
- Quantity: Set this parameter based on the number of servers. In this example, set the quantity to **1**.
- Specify other parameters as needed.

**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**.

----End

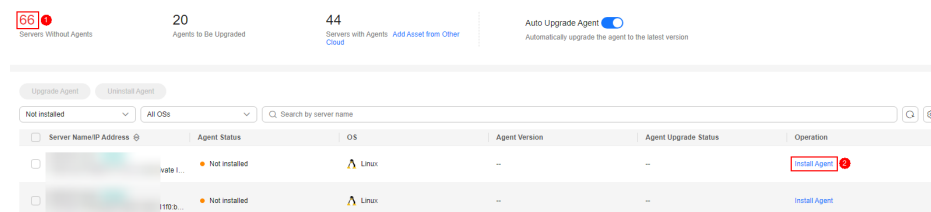
## Step 2: Install an Agent

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

**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

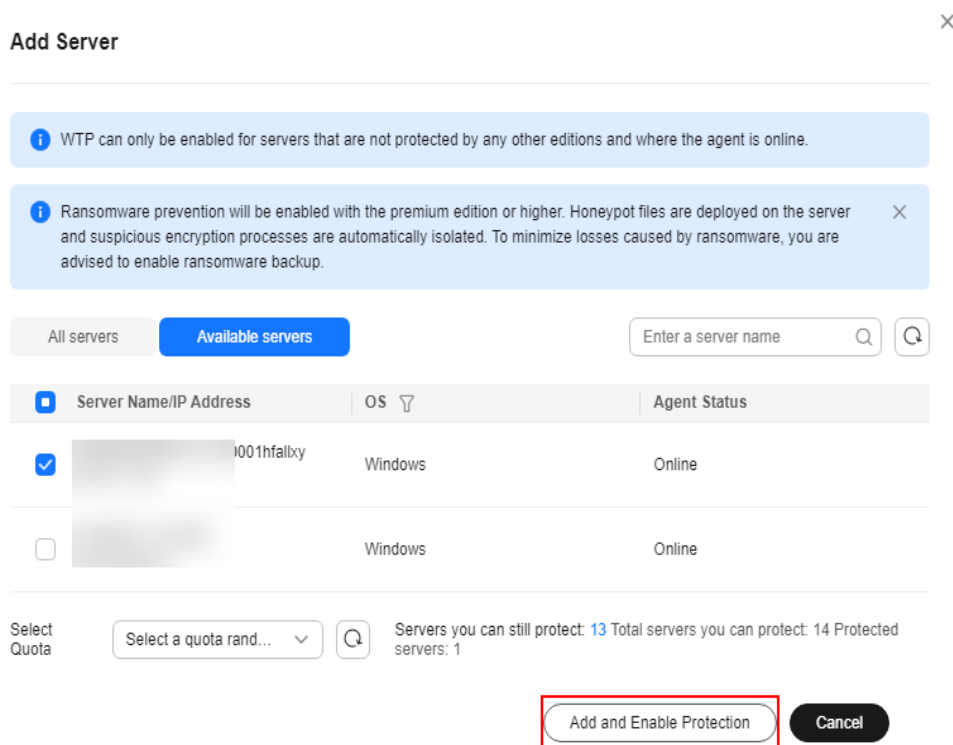
### Step 3: Enable Protection

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

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

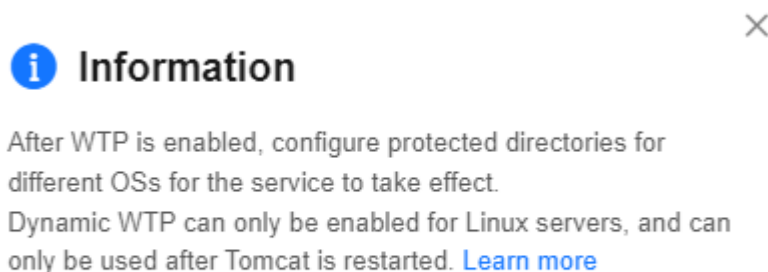
**Step 3** On the **Add Server** page, select the target server and click **Add and Enable Protection**.

**Figure 3-4** Adding a protected server



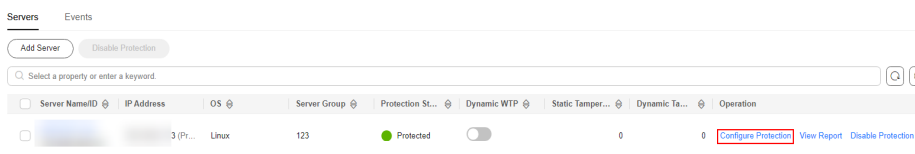
**Step 4** Read the message for adding a protected directory and click **X**.

**Figure 3-5** Prompt information



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

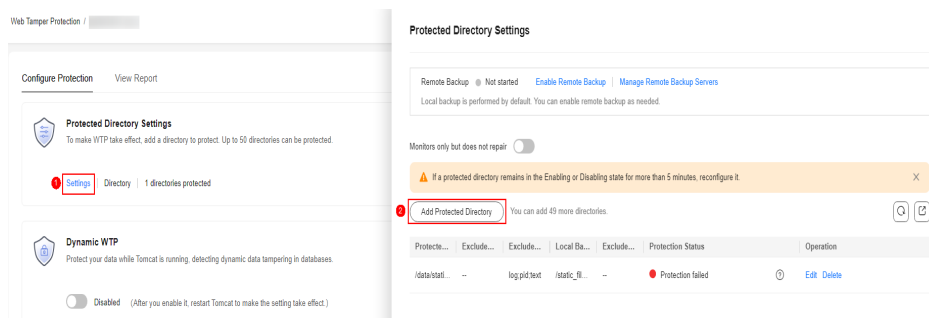
**Figure 3-6** Protection settings



**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 3-7** Adding a protected directory



3. Add protected directories based on service requirements. For details about the parameters, see [Table 3-1](#).

**Table 3-1** Parameters for adding a protected directory

Parameter	Description	Example Value
Protected Directory	Add directories to be protected. <ul style="list-style-type: none"> <li>– Do not add an OS directory as a protected directory.</li> <li>– After a directory is added, the files and folders in the protected directory are read-only and cannot be modified directly.</li> </ul>	/etc/lesuo
Excluded Subdirectory	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.	lesuo/test

Parameter	Description	Example Value
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
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"> <li>- The local backup path must be valid and cannot overlap with the protected directory path.</li> <li>- Excluded subdirectories and types of files are not backed up.</li> <li>- Generally, the backup completes within 10 minutes. The actual duration depends on the size of files in the protected directory.</li> <li>- 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.</li> </ul>	/etc/backup

Parameter	Description	Example Value
Excluded File Path	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 (/).	lesuo/data;lesuo/list

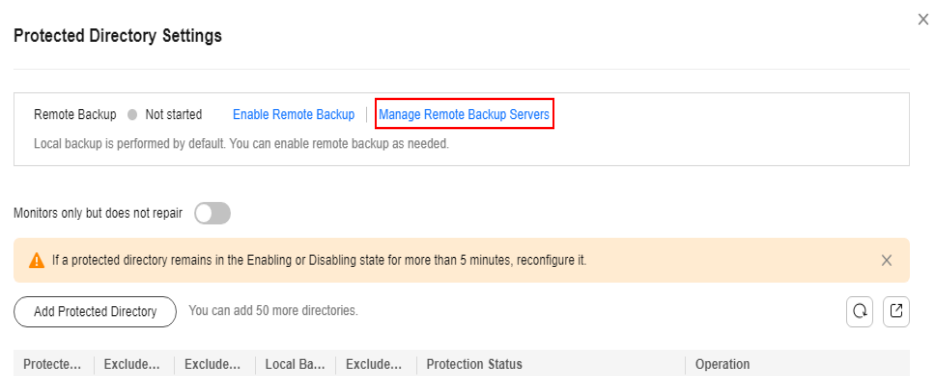
4. Click **OK**.
5. In the protected directory list, if **Protection Status** is **Protected**, the directory is added successfully.

**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 3-8** Managing remote backup servers



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

**Table 3-2** Backup server parameters

Parameter	Description	Example Value
Server Name	Name of the remote backup server.	test

Parameter	Description	Example Value
Address	Enter the private IP address of the Huawei Cloud server as the remote backup 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
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"><li>- 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 <b>/hss01</b> and <b>hss02</b>, and the agent IDs of the two servers are <b>f1fdbabc-6cdc-43af-acab-e4e6f086625f</b> and <b>f2ddbabc-6cdc-43af-abcd-e4e6f086626f</b>, and the remote backup path is <b>/hss01</b>. The corresponding backup paths are <b>/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f</b> and <b>/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f</b>.</li><li>- 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.</li></ul>	<b>/f1fdbabc-6cdc-43af-acab-e4e6f086625f</b>

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.

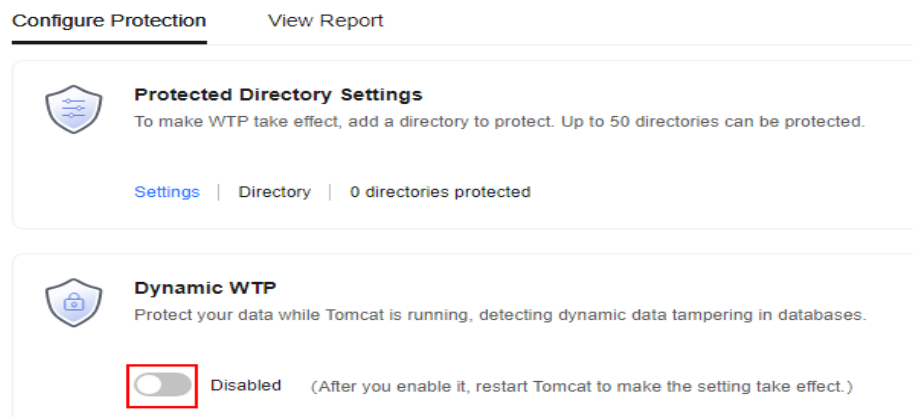
**Step 8** (Optional) Enable dynamic WTP.



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 3-9** Enable dynamic WTP



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 3-3](#) describes the functions.

**Table 3-3** Proactive server protection functions

Function	Description
<b>Ransomware Prevention</b>	<p>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.</p> <p>Ransomware prevention is automatically enabled with the WTP edition. Honeypot files are deployed on your server and suspicious encryption programs are automatically isolated. You can modify the ransomware protection policy. You are also advised to enable backup so that you can restore data.</p>
<b>Application Protection</b>	<p>To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.</p>
<b>Application Processes Control</b>	<p>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.</p>
<b>Virus scanning and removal</b>	<p>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.</p>

# 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 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 purchase and enable container security protection.

## 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.

- **Billing Mode:** Select a billing mode as required. In this example, select **Yearly/Monthly**.
- **Region:** Select the region where the server is located. In this example, select **CN-Hong Kong**.
- **Edition:** Select **Container**.
- **Quantity:** Set this parameter based on the number of container nodes. In this example, set the quantity to **1**.
- Specify other parameters as needed.

**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**.

----End

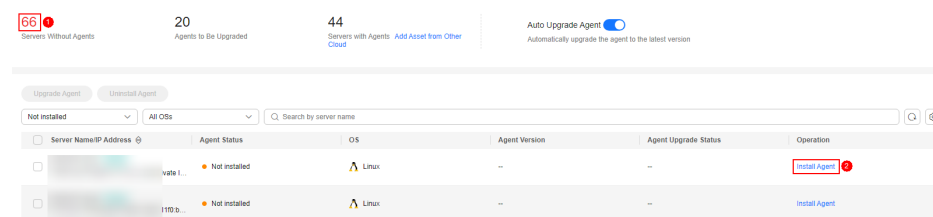
## Step 2: Install an Agent

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

**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 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.

Set this parameter based on the edition of the purchased quota in **Step 1: Purchase HSS Quota**.

- **Billing Mode:** Select **Yearly/Monthly**.
- **Edition:** Select **Container**.

**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 4-4** 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 9/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 4-1** describes the functions.

**Table 4-1** Container node protection functions

Function	Description
<b>Container image security scanning</b>	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.
<b>Ransomware Prevention</b>	<p>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.</p> <p>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.</p>
<b>Application Protection</b>	To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.
<b>Application Processes Control</b>	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.
<b>Virus scanning and removal</b>	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.
<b>Container Cluster Protection</b>	<p>HSS can check for non-compliance baseline issues, vulnerabilities, and malicious files when a container image is started and report alarms on or block container startup that has not been unauthorized or may incur high risks.</p> <p>You can configure container cluster protection policies to block images with vulnerabilities, malicious files, non-compliant baselines, or other threats, hardening cluster security.</p>



Function	Description
<b>Container Firewall</b>	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

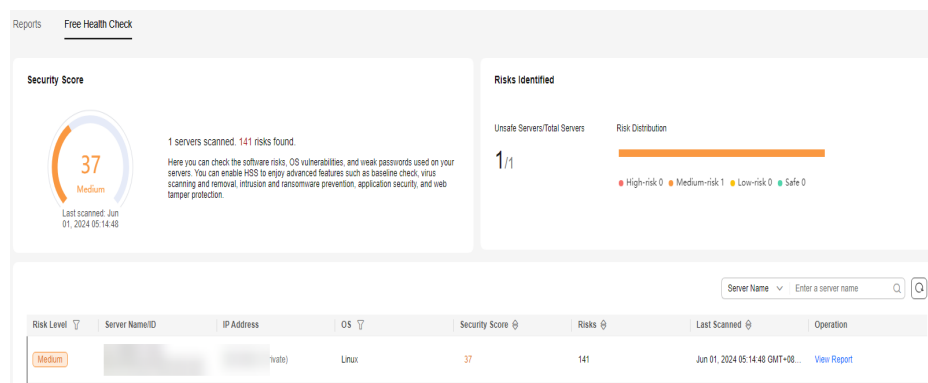
ECSs that are not protected by HSS are scanned for free in the early morning on each Monday. This section describes how to view the security situation of ECSs that are not protected by HSS.

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 and choose **Security & Compliance > Host Security Service**. The HSS console is displayed.
- 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



- **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.

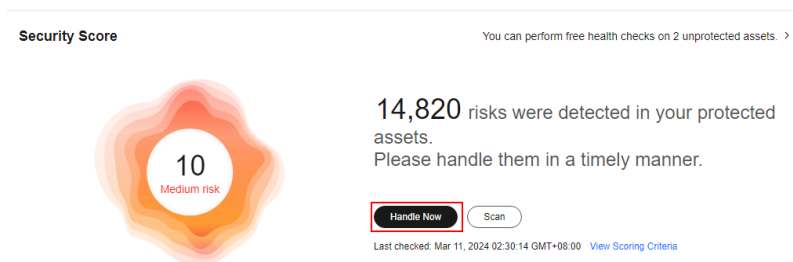
**Step 3** Click  in the upper left corner and choose **Security & Compliance > Host Security Service**. The HSS console is displayed.


**Step 4** View the ECS security situation.

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



- In the **Handle Now** dialog box, click  to view risk details.
  - Click **Handle** to go to the risk details page and view and handle security risks.
- View the security risk distribution and trend.
    - 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	Risks
...	Running	Online	Protected	Risky	Assets: 0 Vulnerabilities: 174 Unsafe Settings: 53 Intrusions: 0
... (.165/Private IP)	Running	Offline	Protection interrupted	Risky	

- 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	<a href="#">Best Practices of Login Security Hardening</a>	HSS login protection greatly improves server security.
Vulnerability fixing	<a href="#">Git Credential Disclosure Vulnerability (CVE-2020-5260)</a>	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.
	<a href="#">SaltStack Remote Command Execution Vulnerabilities (CVE-2020-11651 and CVE-2020-11652)</a>	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><b>OpenSSL High-risk Vulnerability (CVE-2020-1967)</b></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><b>Adobe Font Manager Library Remote Code Execution Vulnerability (CVE-2020-1020/ CVE-2020-0938)</b></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><b>Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027)</b></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><b>Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)</b></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	<a href="#">HSS multi-cloud management</a>	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	<a href="#">Best Practices for Defense Against Ransomware</a>	<p>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.</p> <p>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.</p>
Web tamper protection	<a href="#">Combining WAF and HSS to Get Improved Web Tamper Protection</a>	With HSS and WAF in place, you can stop worrying about web page tampering.