Host Security Service

User Guide

Issue	25
Date	2025-07-04

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Using IAM to Grant Access to HSS

1.1 Creating a User and Granting Permissions

This section describes IAM's fine-grained permissions management for your HSS resources. With **IAM**, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to HSS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei cloud account or cloud service to perform professional and efficient O&M on your HSS resources.

If your Huawei Cloud account does not require individual IAM users, skip this chapter.

This section describes the procedure for granting permissions (see **Figure 1-1**).

Prerequisite

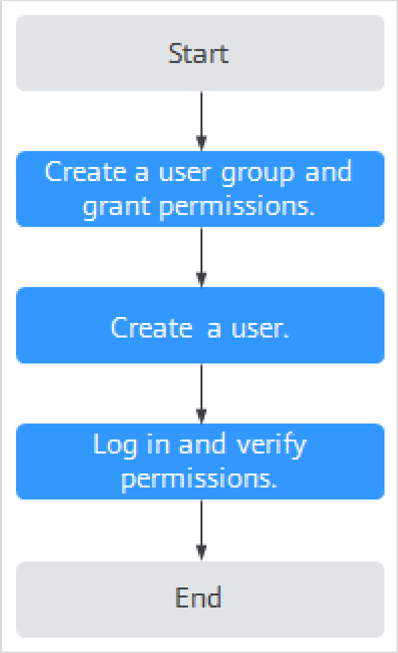
Before authorizing permissions to a user group, you need to know which HSS permissions can be added to the user group. **Table 1-1** describes the policy details.

Table 1-1 System-defined permissions supported by HSS

Role/Policy Name	Description	Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS	System-defined role	● It depends on the **Tenant Guest** role. Tenant Guest: A global role, which must be assigned in the global project. ● To purchase HSS protection quotas, you must have the **ECS ReadOnlyAccess**, **BSS Administrator**, and **TMS ReadOnlyAccess** roles. – **ECS ReadOnlyAccess**: read-only access permission for the ECS. This is a system policy. – **BSS Administrator**: a system role, which is the administrator of the billing center (BSS) and has all permissions for the service. – **TMS ReadOnlyAccess**: a system-defined policy that grants read-only access to TMS.
HSS FullAccess	All HSS permissions	System-defined policy	To purchase HSS protection quotas, you must have the **BSS Administrator** role. **BSS Administrator**: a system role, which is the administrator of the billing center (BSS) and has all permissions for the service. **SMN ReadOnlyAccess**: a system-defined policy that grants read-only access to SMN.
HSS ReadOnlyAccess	Read-only permission for HSS	System-defined policy	**SMN ReadOnlyAccess**: a system-defined policy that grants read-only access to SMN.

Authorization Process

Figure 1-1 Process for granting permissions


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

The following procedure describes how to grant only the **HSS Administrator** permission to users, so that the users can only access and manage HSS and cannot access other cloud services.

1. **Create a user group and assign permissions**. On the IAM console, grant the **HSS Administrator** permission.
2. **Create a user and add it to the group**. On the IAM console, add the user to the group created in **1**.
3. **Log in** and verify permissions.

   Log in to the management console as the new user, switch to a region where the user has been granted permissions, and verify that the user only has the **HSS Administrator** permission.

   a. In the service list, choose HSS. The **Dashboard** page is displayed.
   b. Choose a service other than HSS from the service list. A message is displayed indicating that the user does not have the permission.

   The **HSS Administrator** permission has taken effect.

1.2 HSS Custom Policies

Custom policies can be created to supplement the system-defined policies of HSS. For details about the actions supported by custom policies, see **HSS Actions**.

You can create custom policies using one of the following methods:

- Visual editor: Select cloud services, actions, resources, and request conditions. You do not need to have knowledge of the policy syntax.

- JSON: Create a policy in JSON format or edit the JSON strings of an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common HSS custom policies.

Example Custom Policies

- Example 1: Allowing users to query the protected server list

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:list"
                                                        ]
                }
        ]
}
```

- Example 2: Denying agent uninstallation

  A deny policy must be used together with other policies. If the policies assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **HSS Administrator** policy to a user but also forbid the user from deleting key pairs (**hss:agent:uninstall**). Create a custom policy with the action to delete key pairs, set its **Effect** to **Deny**, and assign both this and the **HSS Administrator** policies to the group the user belongs to. Then the user can perform all operations on HSS except uninstalling it. The following is an example policy that denies agent uninstallation.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Deny",
                        "Action": [
                                "hss:agent:uninstall"
                        ]
                },
        ]
}
```

- Multi-action policies

  A custom policy can contain the actions of multiple services that are of the project-level type. The following is a policy with multiple statements:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:list"
                        ]
                },
               {
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:switchVersion",
                                "hss:hosts:manualDetect",
                                "hss:manualDetectStatus:get"
                        ]
        }
    ]
}
```

1.3 HSS Actions

This section describes fine-grained permissions management for your HSS instances. If your Huawei Cloud account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign policies or roles to these groups. The user then inherits permissions from the groups it is a member of. This process is called authorization. After authorization, the user can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using **roles** and **policies**. Roles are provided by IAM to define service-based permissions depending on user's job responsibilities. IAM uses policies to perform fine-grained authorization. A policy defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

HSS provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. The following are related concepts:

- Permissions: Allow or deny certain operations.
- Actions: Specific operations that are allowed or denied.
- Dependent actions: When assigning permissions for an action, you also need to assign permissions for the dependent actions.

HSS supports the following actions that can be defined in custom policies:

Actions describes the HSS actions, such as querying the HSS list, enabling or disabling HSS for a server, and manual detection.

Actions

Permission	Action	Related Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Query asset information	hss:assets:list	-	√	×
Delete a cluster protection policy	hss:clusterProtect:delete	-	√	×

Permission	Action	Related Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Configure a runtime application self-protection policy	hss:rasp:set	-	√	×
Configure asset importance	hss:hosts:set	-	√	×
Manage associated assets	hss:assets:set	-	√	×
Query image information	hss:images:list	-	√	×
Query runtime application self-protection details	hss:rasp:list	-	√	×
Configure a security check	hss:securitycheck:set	-	√	×
Query cluster protection status	hss:clusterProtect:list	-	√	×
Batch-scan images	hss:images:set	-	√	×
Configure a cluster protection policy	hss:clusterProtect:set	-	√	×
Check backup status	hss:antiransomware:list	-	√	×
Configure a backup policy	hss:antiransomware:set	-	√	×
Query security check results	hss:securitycheck:list	-	√	×
Display container assets	hss:containers:get	-	√	×
Configure the overview	hss:overview:set	-	√	×
Query the Application Recognition Service (ARS) list	hss:ars:list	-	√	×
Check the overview	hss:overview:list	-	√	×

Permission	Action	Related Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Configure a report	hss:report:set	-	√	×
Querying a report	hss:report:list	-	√	×
Install the agent	hss:installAgent:set	-	√	×
Query the programs that have been automatically isolated and killed	hss:automaticKillMp:get	-	√	×
Query weak passwords	hss:weakPwds:get	-	√	×
Query the account list	hss:accounts:list	-	√	×
Configure WTP alarms	hss:wtpAlertConfig:set	-	√	×
Perform batch operations on web shells	hss:webshells:operate	-	√	×
Configure scheduled protection	hss:wtpScheduledProtections:set	-	√	×
Query common login IP addresses	hss:commonIPs:list	-	√	×
Configure server groups	hss:hostGroup:set	-	√	×
Perform batch operations on malicious programs	hss:maliciousPrograms:operate	-	√	×
Query web shell scan results	hss:webshells:list	-	√	×
Update container network information	hss:container-network:set	-	√	×

Permission	Action	Related Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Query the protected file system list	hss:wtpFilesystems:list	-	√	×
Query the open port list	hss:ports:list	-	√	×
Query the process list	hss:processes:list	-	√	×
Configure protected directories	hss:wtpDirectorys:set	-	√	×
Query password complexity policy scan reports	hss:complexityPolicys:list	-	√	×
Query risky account scan reports	hss:riskyAccounts:list	-	√	×
Query the detected intrusion list	hss:event:get	-	√	×
Querying container assets	hss:containers:list	-	√	×
Query yearly/monthly quotas	hss:quotas:get	-	√	×
Query WTP alarms	hss:wtpAlertConfig:get	-	√	×
Configure backup servers	hss:wtpBackup:set	-	√	×
Unblock an IP address that was blocked during account cracking prevention	hss:accountCracks:unblock	-	√	×
Query the protection mode	hss:wtpProtectMode:get	-	√	×
Query the vulnerability list	hss:vuls:list	-	√	×

Permission	Action	Related Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Configure a protected file system	hss:wtpFilesystems:set	-	√	×
Enable 2FA	hss:twofactorAuth:set	-	√	×
Query server groups	hss:hostGroup:get	-	√	×
Query the software list	hss:softwares:list	-	√	×
Perform operations on vulnerabilities	hss:vuls:set	-	√	×
Edit baseline data	hss:baselines:set	-	√	×
Perform batch operations on open ports	hss:ports:operate	-	√	×
Perform operations on intrusions	hss:event:set	-	√	×
Query the privileged process list	hss:wtpPrivilegedProcesses:list	-	√	×
Query configuration scan reports	hss:configDetects:list	-	√	×
Query the login IP address whitelist	hss:whiteIps:list	-	√	×
Query HSS alarms	hss:alertConfig:get	-	√	×
Perform batch operations on vulnerabilities	hss:vuls:operate	-	√	×
Query backup servers	hss:wtpBackup:get	-	√	×
Obtain server risk statistics	hss:riskyDashboard:get	-	√	×

Permission	Action	Related Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Subscribe to a security report	hss:safetyReport:set	-	√	×
Query the protected server list	hss:hosts:list	ecs:cloudServers:list vpc:ports:get vpc:publicIps:list	√	×
Manage container assets	hss:containers:set	-	√	×
Query security reports	hss:safetyReport:list	-	√	×
Configure weak passwords	hss:weakPwds:set	-	√	×
Query malicious program scan results	hss:maliciousPrograms:list	-	√	×
Query container network information	hss:container-network:read	-	√	×
Purchase a quota	hss:quotas:set	-	√	×
Enable or disable WTP	hss:wtpProtect:switch	-	√	×
Configure HSS alarms	hss:alertConfig:set	-	√	×
Perform operations on detected unsafe settings	hss:configDetects:operate	-	√	×
Configure web paths	hss:webDirs:set	-	√	×
Configure the login IP address whitelist	hss:whiteIps:set	-	√	×
Query web paths	hss:webDirs:get	-	√	×

Permission	Action	Related Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Enable or disable protection on servers	hss:hosts:switchVersion	-	√	×
Uninstall an agent	hss:agent:uninstall	-	√	×
Configure ARS	hss:ars:set	-	√	×
Obtain the list of servers where 2FA is enabled	hss:twofactorAuth:list	-	√	×
Manual scan	hss:hosts:manualDetect	-	√	×
Query weak password scan reports	hss:weakPwds:list	-	√	×
Query Application Recognition Service (ARS)	hss:ars:get	-	√	×
Query WTP statistics	hss:wtpDashboard:get	-	√	×
Query the agent download address	hss:installAgent:get	-	√	×
Query important file change reports	hss:keyfiles:list	-	√	×
Query account cracking protection reports	hss:accountCracks:list	-	√	×
Query common login locations	hss:commonLocations:list	-	√	×
Query remote login scan results	hss:abnorLogins:list	-	√	×
Query policy group	hss:policy:get	-	√	×
Query the web path list	hss:webdirs:list	-	√	×
Query scheduled protection	hss:wtpScheduledProtections:get	-	√	×

Permission	Action	Related Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Query the WTP list	hss:wtpHosts:list	ecs:cloudServers:list vpc:ports:get vpc:publicIps:list	√	×
Query baseline data	hss:baselines:list	-	√	×
Query the protected directory list	hss:wtpDirectorys:list	-	√	×
Check the status of a manual scan	hss:manualDetectStatus:get	-	√	×
Configure common login IP addresses	hss:commonIPs:set	-	√	×
Query the container network list	hss:container-network:list	-	√	×
Configure a protection mode	hss:wtpProtectMode:set	-	√	×
Query the auto-startup list	hss:launch:list	-	√	×
Configure common login locations	hss:commonLocations:set	-	√	×
Configure privileged processes	hss:wtpPrivilegedProcess:set	-	√	×
Query WTP records	hss:wtpReports:list	-	√	×
File integrity check	hss:keyfiles:set	-	√	×
Configure a policy group	hss:policy:set	-	√	×

Permission	**Action**	**Related Action**	**IAM Project** **(Project)**	**Enterprise Project** **(Enterprise Project)**
Enable or disable automatic isolation and killing of malicious programs	hss:automaticKillMp:set	-	√	×

2 Accessing HSS

2.1 Access Overview

Figure 2-1 shows the process of accessing and enabling HSS.

Figure 2-1 HSS access process

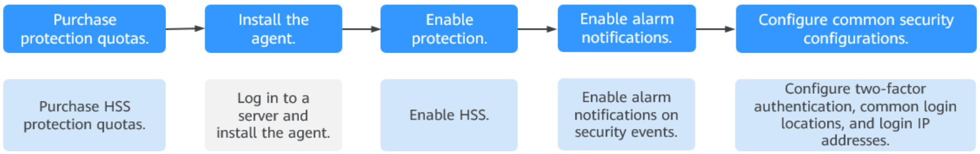

Purchase protection quotas.
Install the agent.
Enable protection.
Enable alarm notifications.
Configure common security configurations.
Purchase HSS protection quotas.
Log in to a server and install the agent.
Enable HSS.
Enable alarm notifications on security events.
Configure two-factor authentication, common login locations, and login IP addresses.

Table 2-1 Description of the HSS access process

No.	Step	Description
1	**Purchasing Protection Quotas**	HSS provides the basic, professional, enterprise, premium, web tamper protection, and container editions. Each edition supports different functions and features. You need to purchase the corresponding edition based on your protection requirements for servers or containers. For details about the differences between the editions of the HSS, see **Features**.
2	**Installing the Agent**	The HSS agent is a piece of software installed on cloud servers to exchange data between the servers and HSS, implementing security detection and protection. You can use only after installing the agent.
3	**Enabling Protection**	You need to enable protection for your ECSs.

No.	Step	Description
4	Enabling Alarm Notifications	By default, security risks detected by HSS are displayed on the management console. You need to log in to the console and view the risks. If you want to know the security risks of servers or containers in a timely manner, you can enable the alarm notification function. After the function is enabled, HSS will send security risks to you by SMS or email.
5	Common Security Configurations	To improve ECS security, you can configure the following ECS security protection items based on your service requirements: ● Common login locations: HSS allows users to log in to ECSs in common login locations and generates alarms when users log in to ECSs in non-common login locations. ● Common login IP address: HSS allows common login IP addresses to log in to ECSs and generates alarms for uncommon login IP addresses. ● SSH login IP address whitelist: HSS only allows IP addresses in the whitelist to log in to ECSs using SSH. ● Two-factor authentication: The two-factor authentication mechanism is used together with the SMS or email verification code to perform secondary authentication on ECS login. ● Isolation and killing of malicious programs: HSS automatically isolates and kills identified malicious programs, such as backdoors, Trojans, and worms.

2.2 Purchasing an HSS Quota

You can purchase an HSS quota on the console.

Precautions

- The quota can be used only in the region where you bought it.
- A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- Currently, HSS can only protect Docker, Containerd, CRI-O, Podman, and iSulad containers. Check your container type before purchasing the container edition.
- The **enterprise edition** is no longer sold. You are advised to purchase the **premium edition** to protect your servers.
- HSS should be deployed on all your servers so that if a virus infects one of them, it will not be able to spread to others and damage your entire network.
- After purchasing quota, go to the **Servers & Quota** page to enable HSS.

Regions

Table 2-2 Choosing a region to purchase HSS

Server	Server Region	Region
- ECS - BMS - HECS - Huawei Cloud Workspace	Regions where HSS is available	Regions where your ECSs/BMSs/HECSs/ Workspaces are deployed HSS cannot be used across regions. If the server and your protection quota are in different regions, unsubscribe from the quota and purchase a quota in the region where the server is deployed.
Third-party cloud server	-	Currently, only some regions support access to non-Huawei Cloud servers. For details about the regions, see **In What Regions Is HSS Available to Non-Huawei Cloud Servers?** Purchase an HSS quota in the region that supports non-Huawei Cloud servers. Connect the server to the region by performing the installation procedure for non-Huawei Cloud servers.
On-premises IDCs	-	

Prerequisites

The account must have the **BSS Administrator** and **HSS Administrator** permissions. If the account does not have the permissions, use a management account to purchase quotas or authorize member accounts to purchase quotas. For details about authorization, see **Creating a User and Granting Permissions**.

Purchasing an HSS Quota

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

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the upper right corner of the **Overview** page, click **Buy HSS**.

Step 4 On the **Buy HSS** page, set the quota specifications.

Table 2-3 Parameters for purchasing HSS

Parameter	Description	Example Value
Region	- You are advised to purchase quota in the region of your servers. - HSS cannot be used across regions. If you purchased a quota in a wrong region, unsubscribe from it and purchase a quota in the region of your servers. - Only some regions allow non-Huawei Cloud servers to access HSS through the Internet. For details, see **In What Regions Is HSS Available to Non-Huawei Cloud Servers?** Purchase HSS in the regions where non-Huawei Cloud servers can be connected.	CN-Hong Kong
Billing Mode	Select **Yearly/Monthly** or **Pay-per-use** billing mode based on your requirements. - **Yearly/Monthly**: You can buy a yearly or monthly subscription. It is 30% cheaper than the pay-per-use mode for the same service duration. If you plan to use HSS for a long time, you are advised to choose this mode. It supports the HSS basic, professional, premium, WTP, and container editions. - **Pay-per-use**: You pay for the duration you use the resources. Prices are calculated by hour, and no minimum fee is required. This billing mode supports the HSS professional, premium, container, and WTP editions. **NOTE** Procedure for enabling pay-per-use quota: 1. On the purchase page, select **Pay-per-use**. In the lower right corner, click **Enable Now**. You will be redirected to the server list. 2. In the **Operation** column of a server, click **Enable**. Set **Billing Mode** to **Pay-per-use** and select an edition. 3. After confirming the information, select **I have read and agree to the Host Security Service Disclaimer**. 4. Click **OK**.	Yearly/Monthly
Edition	The **basic, professional, premium,WTP,** and **container editions** are supported. For details about the differences between editions, see **Editions**.	Professional Edition
Value-added Services	Container image scans are billed per use. If you need to scan repository and CI/CD images, enable this function. You will be charged per successful scan per image.	Selected

Parameter	Description	Example Value
Enterprise Project	This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects. To enable this function, contact your customer manager. An enterprise project provides a cloud resource management mode, in which cloud resources and members are centrally managed by project. Select an enterprise project from the drop-down list. **NOTE** - 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 displayed in the default enterprise project.	default
Tag	Tags are used to identify cloud resources. When you have many cloud resources of the same type, you can use tags to classify cloud resources by dimension (for example, by usage, owner, or environment). To use this function, your account must have the **TMS administrator** permission. Without this permission, you cannot add tags to protection quotas, and the error message "permission error" will be displayed. You do not need to set this parameter in pay-per-use mode.	data
Quota Management	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. - 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. If you use enterprise projects, this configuration only enables automatic quota binding for the selected enterprise project.	Selected

Parameter	Description	Example Value
Required Duration	- Select a duration based on your requirements. In **Pay-per-use** mode, you do not need to select a duration. - You are advised to select **Auto-renew** to ensure your servers are always protected. - 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. - If you do not select **Auto-renew**, manually renew the service before it expires.	1 year
Quantity	Set the quantity according to the number of server or container nodes to be protected. This parameter is not required in the **Pay-per-use** mode.	20

Step 5 In the lower right corner of the page, click **Next**.

For details about pricing, see **Product Pricing Details**.

Step 6 After confirming that the order, select **I have read and agree to the Host Security Service Disclaimer** and click **Pay Now**.

Step 7 Click **Pay Now** and complete the payment.

Return to the HSS console, choose **Asset Management** > **Servers & Quota**, click the **Quotas** tab, and check the purchased quota.

----End

Follow-up Procedure

After the quota purchase is complete, install the agent on the server or container node.

- For details about how to install the agent on a server or a single container node, see **Installing the Agent on Servers**.
- For details about how to install the agent on a cluster, see **Installing an Agent in a Cluster**.

Related Operations

If you purchased HSS in the wrong edition or region, you can first unsubscribe from it and then purchase the correct quota.

2.3 Installing the Agent on Servers

2.3.1 Agent Overview

What Is an Agent?

The HSS agent is a piece of software installed on cloud servers to exchange data between the servers and HSS, implementing security detection and protection for servers and containers. If no agent is installed, the HSS is unavailable.

Scans all servers at 00:00 every day; monitors the security and monitors status of servers; and reports the collected server and monitors information (including non-compliant configurations, insecure configurations, intrusion traces, software list, port list, and process list) to the cloud protection center. In addition, the agent blocks attacks targeted at servers and containers based on the security policies you configured.

Supported OSs

Currently, some mainstream OSs are supported. For details, see **Supported OSs**. To obtain better HSS service experience, you are advised to install or upgrade to an OS version supported by the agent.

Processes When the Agent Is Running

- **Linux**

  The account of the agent is **root**. **Table 2-4** lists the running processes on a Linux server.

Table 2-4 Agent running process on a Linux server

Agent Process Name	Function	Path
hostguard	Detects security issues, protects the system, and monitors the agent.	/usr/local/hostguard/bin/hostguard
hostwatch	Monitors the agent process.	/usr/local/hostguard/bin/hostwatch
upgrade	Upgrades the agent.	/usr/local/hostguard/bin/upgrade

- **Windows**

  The account of the agent is **system**. **Table 2-5** lists the running processes on a Windows server.

Table 2-5 Agent running process on a Windows server

Agent Process Name	Function	Path
hostguard.exe	Detects security issues, protects the system, and monitors the agent.	C:\Program Files\HostGuard\HostGuard.exe
hostwatch.exe	Monitors the agent process.	C:\Program Files\HostGuard\HostWatch.exe
upgrade.exe	Upgrades the agent.	C:\Program Files\HostGuard\upgrade.exe

Installing the Agent

1. Check the installation environment.

   Before installing the agent, perform the operations in **Checking the Installation Environment**.

2. Install the agent.

   The procedure for installing the agent varies according to the server type. For details, see:

   – **Installing the Agent on Huawei Cloud Servers**

   – **Installing the Agent on Third-party Servers**

2.3.2 Checking the Installation Environment

Agent installation has restrictions on security group outbound ports, DNS server addresses, and third-party security software. Before installing it, perform the operations in **Checking the Installation Environment** to ensure the installation requirements are met.

Checking the Installation Environment

Step 1 Ensure your server OS is supported by the agent. For more information, see the table in **Supported OSs**.

The agent cannot be installed on the OSs that are not in the list.

Step 2 Ensure the server is running properly.

The agent cannot be installed if the server is not running.

Step 3 Ensure the capacity of the disk where the agent is to be installed is greater than 300 MB.

If the available space is less than 300 MB, the agent will fail to be installed. The agent installation path cannot be customized. The following default paths are used:

- Linux: **/usr/local/hostguard/**
- Windows: **C:\Program Files\HostGuard**

Step 4 Check whether mandatory ports are enabled in the server security group.

- Huawei Cloud servers

  For servers in regions other than **CN East 2** and **CN Southwest-Guiyang1**, 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.) This port is used to communicate with the HSS server. For details about how to view and modify an outbound ECS security group rule, see **Modifying a Security Group**.

- Third-party cloud servers

  Ensure the outbound rule of your security group allows access to port 10180 on the 100.125.0.0/16 CIDR block. (This is the default setting.) This port is used to communicate with the HSS server.

Step 5 Ensure the DNS address of the server is a private DNS server address on the Huawei Cloud.

The agent cannot be downloaded to a private DNS server address outside Huawei Cloud.

For details about how to view and change the DNS server address, see **Modifying the DNS (on the Server)** or **Modifying the DNS Server Address (on the Console)**.

Step 6 Uninstall third-party security software.

Third-party security software will probably be incompatible with the HSS agent and affects HSS protection. If third-party security software is installed on your servers, uninstall it before installing the HSS agent.

Step 7 (Optional) For a Linux server, disable the SELinux firewall.

The SELinux firewall may disrupt agent installation. You can enable it after the agent is successfully installed.

Step 8 (Optional) For Windows, ensure Microsoft Office has been installed on the server and can open the .xlsx file.

----End

Modifying a Security Group

For Huawei Cloud servers, in regions other than **CN East 2** and **CN Southwest-Guiyang1**, 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.) This port is used to communicate with the HSS server. This section describes how to view and modify ECS security group rules.

Step 1 Log in to the management console.

Step 2 In the upper left corner, select a region and a project.

Step 3 Click ☰ in the upper left corner of the management console and choose **Computing** > **Elastic Cloud Server**. The **Elastic Cloud Server** page is displayed.

Step 4 In the ECS list, click the name of an ECS.

Step 5 On the ECS details page, click the **Security Groups** tab and click **Manage Rule**.

Step 6 Click the **Outbound Rules** tab and add a rule, as shown in **Table 2-6**.

Table 2-6 Security group rules

Priority	Action	Type	Protocol & Port		Destination	Description
1	Allow	IPv4	TCP	10180	100.125.0.0/16	Communicates with the HSS server.

----End

Modifying the DNS (on the Server)

When installing the agent, ensure the DNS server address is the Huawei Cloud private DNS server address. This section describes how to view and change the DNS server address on the server.

- Linux server

  The following describes how to add the DNS server address to the **resolv.conf** file using Linux command lines.

  a. Log in to the server as user **root**.

  b. Run the following command to open the **resolv.conf** file:

     vi /etc/resolv.conf

  c. Run the following commands to add the DNS address:

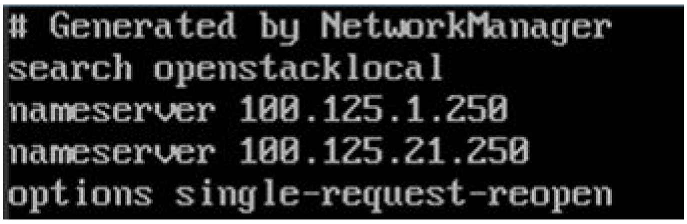
     nameserver *Huawei_Cloud_Private_DNS_server_address*

     NOTE

     The private DNS server addresses vary depending on regions. For details, see **Private DNS Server Address of Huawei Cloud**.

     Take **CN North-Beijing1** as an example. The complete commands are **nameserver 100.125.1.250** and **nameserver 100.125.21.250**.

     Figure 2-2 Adding the DNS server address



```
# Generated by NetworkManager
search openstacklocal
nameserver 100.125.1.250
nameserver 100.125.21.250
options single-request-reopen
```

  d. Press **Esc**, enter **:wq**, and press **Enter** to save the settings and exit.

- Windows server

  The following describes how to use the Windows GUI to add the DNS server address.

a. Log in to the server as the administrator.

b. Choose **Control Panel** > **Network and Sharing Center**, and click **Change adapter settings**.

c. Right-click the network in use and choose **Properties** from the shortcut menu.

d. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.

e. Select **Use the following DNS server addresses** and enter the Huawei Cloud private DNS server address.

NOTE

The private DNS server addresses vary depending on regions. For details, see **Private DNS Server Address of Huawei Cloud**.

Modifying the DNS Server Address (on the Console)

When installing the agent, ensure the DNS server address is the Huawei Cloud private DNS server address. This section uses an ECS as an example to describe how to log in to the console to view and modify DNS configurations.

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Click ≡ in the upper left corner of the management console and choose **Computing** > **Elastic Cloud Server**. The **Elastic Cloud Server** page is displayed.
4. In the ECS list, click the name of an ECS.
5. On the **Summary** tab of the ECS details page, click the VPC name. The **Virtual Private Cloud** page is displayed.
6. Locate the VPC and click the number in the **Subnets** column.
7. Click the name of the subnet.

   In the **Gateway and DNS Information** area, view the DNS server addresses used by the ECS.
8. In the **Gateway and DNS Information** area, click ✎ next to **DNS Server Address**.
9. Change the DNS server addresses to the Huawei Cloud private DNS server addresses.

   NOTE

   The private DNS server addresses vary depending on regions. For details, see **Private DNS Server Address of Huawei Cloud**.

2.3.3 Installing the Agent on Huawei Cloud Servers

Scenario

You can enable HSS for servers only after installing the agent. This section describes how to install the agent on Huawei Cloud servers.

If you use CBH, you can quickly install the agent on the servers through CBH. For details, see **Installing the HSS Agent Using CBH**.

Prerequisites

- The settings of security group outbound ports, DNS server addresses, and third-party security software are appropriate and do not hinder agent installation. You have performed the operations in **Checking the Installation Environment**.
- The VPCOperatePolicy and VPCEPOperatePolicy permissions have been granted to HSS. For details, see **Authorization**.

Constraints

- The HSS agent has been embedded into Workspace images. If you purchase Workspace 23.6.0 or later, the agent will be automatically installed. If your Workspace version is earlier than 23.6.0, you can manually install the agent by referring to this section.
- To install the agent on a target ECS on the HSS console, ensure there is already an executor ECS, which is in the same VPC as the target ECS and has an online HSS agent. If there are no executor ECSs, install the agent on an ECS by referring to **Using the Commands or Script to Install the Agent on Huawei Cloud Servers (Current-Account Installation)**.

Agent Installation Modes

HSS supports two installation modes. For details about their differences, see **Table 2-7**.

Table 2-7 Installation modes

Agent Installation Mode	Description	Scenario	Reference
GUI	It is easy and more efficient than installing the agent using commands. To install the agent in this mode, you simply need to provide HSS with the server username-password pair or key. HSS does not store the password file you upload. Before installation, ensure there is already an executor ECS, which is an ECS with an online agent in the same VPC as the target ECS. If there are no executor ECSs, install the agent on an ECS by referring to **Using the Commands or Script to Install the Agent on Huawei Cloud Servers (Current-Account Installation)**.	There is at least one server with an online agent in the VPC of the servers where the agent is to be installed.	**Installing the Agent on Huawei Cloud Servers on the HSS Console**

Agent Installation Mode	Description	Scenario	Reference
Commands or script	To install the agent using the CLI or script, you need to log in to the server and run commands or a script. This method is more complex and slower than installation on the GUI. The operations for current-account and cross-account installation are as follows: - Current-account installation: The target servers and the HSS quota you purchased are under the same account. You can log in using this account to obtain the installation commands or script and install the agent on the servers. - Cross-account installation: The target servers and the HSS quota you purchased are under different accounts. You can log in to account A to obtain the installation command or script, and install the agent on the target server under account B. After the agent is successfully installed, you can view the target server on the **Asset Management** > **Servers & Quota** page of account A.	- Install the agent for the first time. - There are no servers with an online agent in the VPC of the servers where the agent is to be installed. - Manage and protect servers across accounts.	- **Using the Commands or Script to Install the Agent on Huawei Cloud Servers (Current-Account Installation)** - **Using the Commands or Script to Install the Agent on Huawei Cloud Servers (Cross-Account Installation)**

Installing the Agent on Huawei Cloud Servers on the HSS Console

You can install the agent on servers on the HSS console. Various installation methods are provided below.

Using a Username and Password to Install the Agent on a Huawei Cloud Server

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

Step 8 Configure installation parameters as follows:

- **Install Mode**: Select **GUI**.
- **Server Authentication Mode**: Select **Account and password**.
- **Scale**: Select **Single**.

Step 9 Select a server and click **Next**.

Step 10 Enter a username and password as prompted.

- Linux

  Provide information based on whether the server can be logged in using the **root** account.

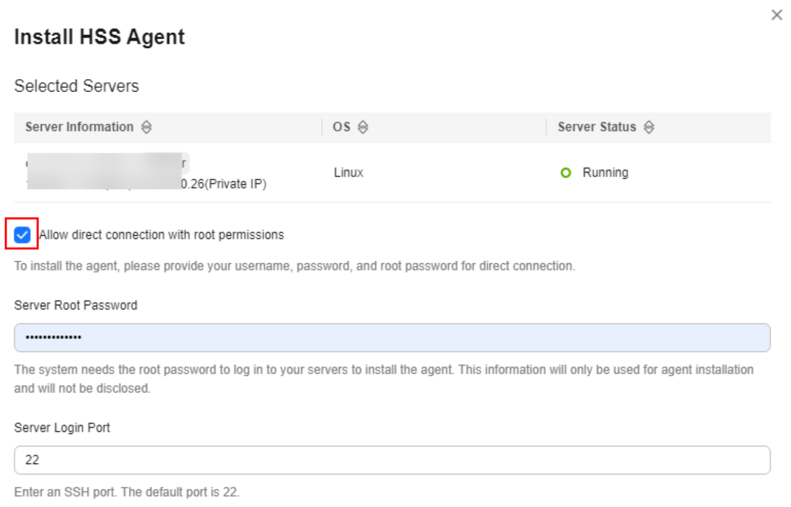
  – If **Allow direct connection with root permissions** is selected:

    The **root** account can be used to log in to the server. Provide the **root** user password and login port. HSS will use your **root** account to install the agent for the server.

  – If **Allow direct connection with root permissions** is not selected:

    The **root** account cannot be used to log in to the server. Provide another username and password for login, and the **root** password for privilege escalation. HSS will use the provided account information to install the agent for the server.

Figure 2-3 Entering the username and password (Linux)



Install HSS Agent

Selected Servers

Server Information	OS	Server Status
[redacted] 0.26(Private IP)	Linux	○ Running

☑ 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

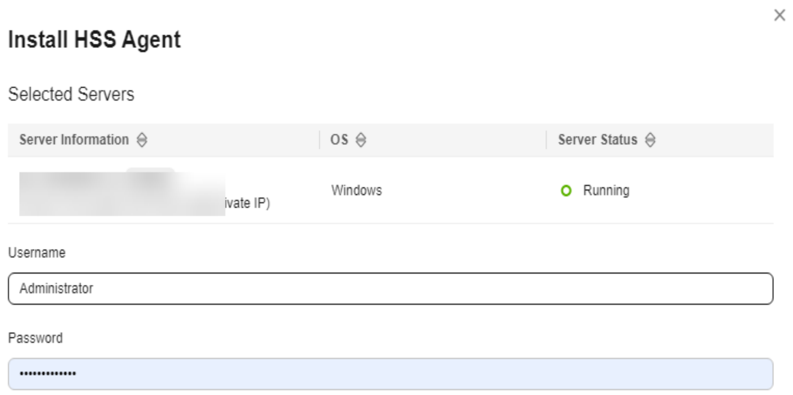
22

Enter an SSH port. The default port is 22.

- Windows

  Enter a username and its password.

Figure 2-4 Entering the username and password (Windows)



Install HSS Agent

Selected Servers

Server Information	OS	Server Status
[redacted] ivate IP)	Windows	○ Running

Username

Administrator

Password

•••••••••••••

Step 11 Confirm the information and click **OK**.

You can view the **Agent Status** column to check the agent installation progress. If the **Agent Status** is **Online**, the agent has been installed.

----End

Using a Username and Password to Install the Agent on Multiple Huawei Cloud Servers

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

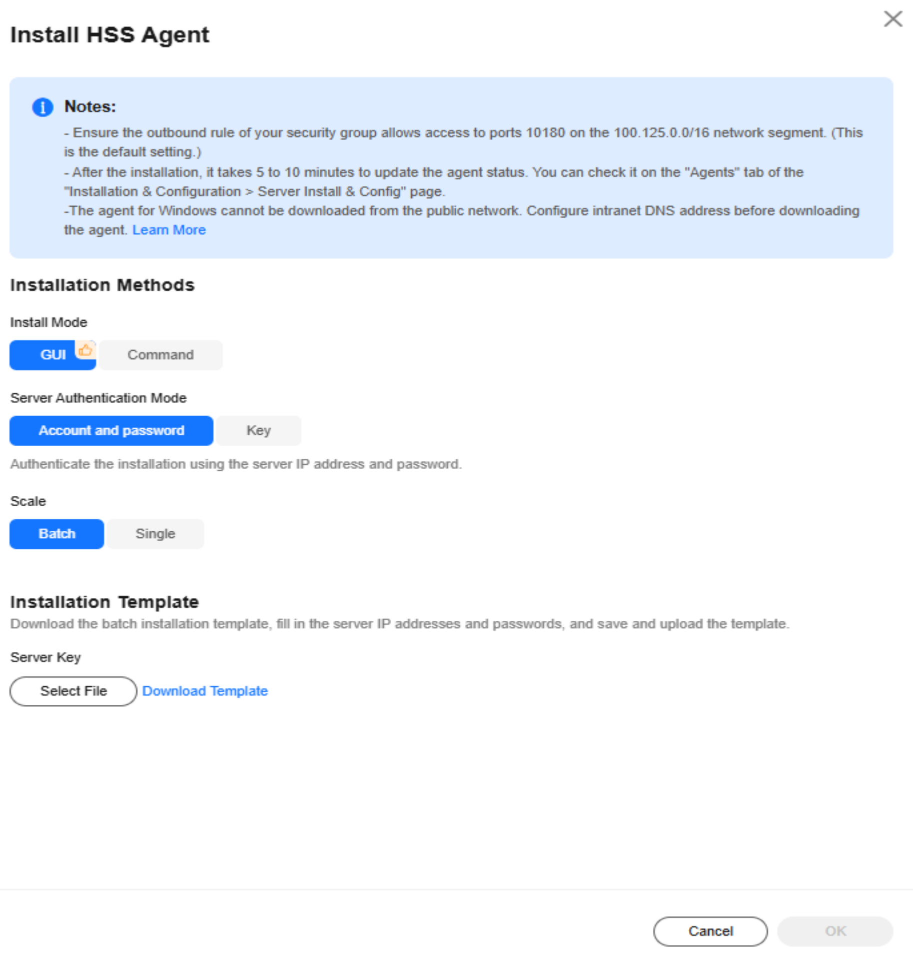
Step 8 Configure installation parameters as follows:

- **Install Mode**: Select **GUI**.
- **Server Authentication Mode**: Select **Account and password**.
- **Scale**: Select **Batch**.

Step 9 Upload the installation template.

1. Click **Download Template** to download the batch installation template to your local PC.

Figure 2-5 Downloading the batch installation template



Install HSS Agent

Notes:
- Ensure the outbound rule of your security group allows access to ports 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Agents" tab of the "Installation & Configuration > Server Install & Config" page.
-The agent for Windows cannot be downloaded from the public network. Configure intranet DNS address before downloading the agent. Learn More

Installation Methods

Install Mode
GUI | Command

Server Authentication Mode
Account and password | Key

Authenticate the installation using the server IP address and password.

Scale
Batch | Single

Installation Template
Download the batch installation template, fill in the server IP addresses and passwords, and save and upload the template.

Server Key
Select File | Download Template

Cancel | OK

2. Open the downloaded file, fill in server information as required, and save the file.
3. Click **Select File** and upload the file.

HSS will automatically parse the file and identify the servers you specified. If the parsing fails, you can click **View Failed Servers** and check the failure cause.

Step 10 Confirm the information and click **OK**.

You can view the **Agent Status** column to check the agent installation progress. If the **Agent Status** is **Online**, the agent has been installed.

----End

Using DEW to Install the Agent on One or Multiple Huawei Cloud Servers

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

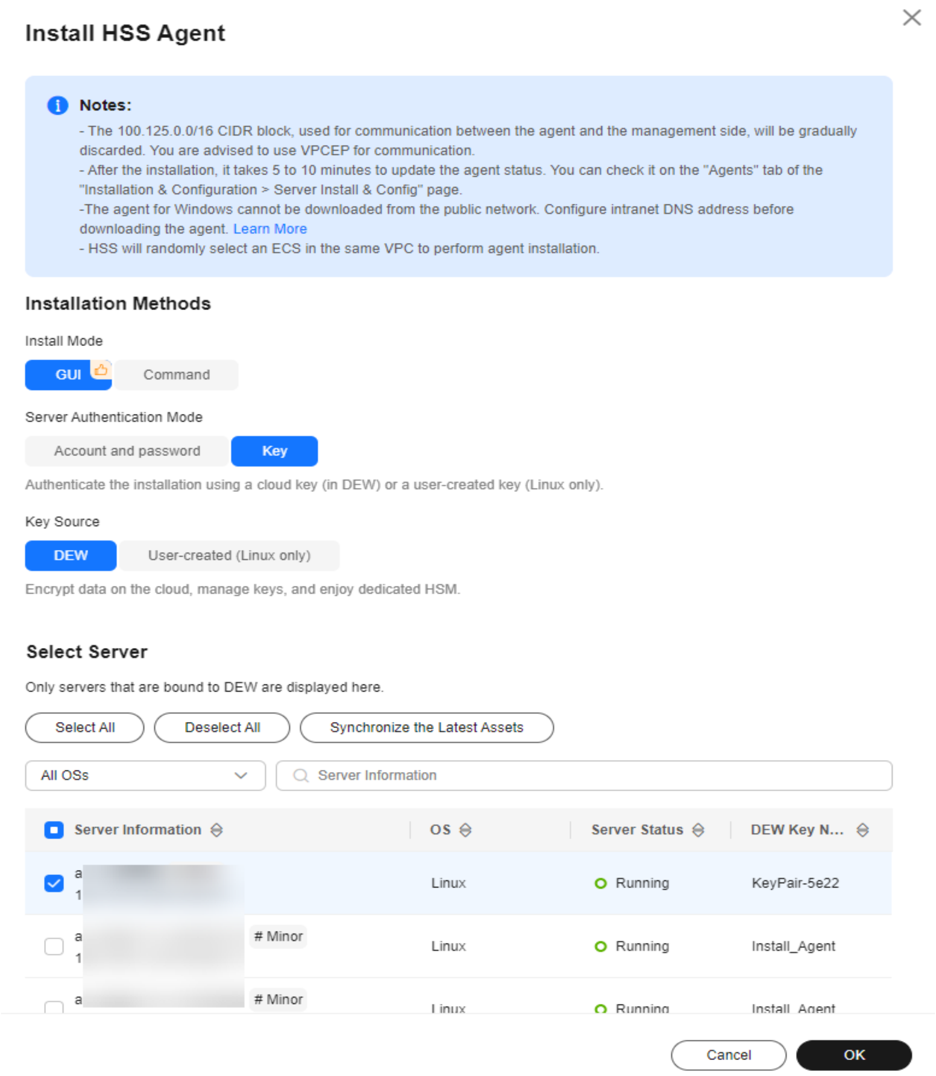
Step 8 Configure installation parameters as follows:

- **Install Mode**: Select **GUI**.
- **Server Authentication Mode**: Select **Key**.
- **Key Source**: Select **DEW**

Step 9 Select servers and click **OK**.

In the server list, only the servers bound to DEW are displayed.

Figure 2-6 Selecting servers



Install HSS Agent

Notes:

- 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.
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Agents" tab of the "Installation & Configuration > Server Install & Config" page.
-The agent for Windows cannot be downloaded from the public network. Configure intranet DNS address before downloading the agent. Learn More
- HSS will randomly select an ECS in the same VPC to perform agent installation.

Installation Methods

Install Mode: GUI | Command

Server Authentication Mode: Account and password | Key

Authenticate the installation using a cloud key (in DEW) or a user-created key (Linux only).

Key Source: DEW | User-created (Linux only)

Encrypt data on the cloud, manage keys, and enjoy dedicated HSM.

Select Server

Only servers that are bound to DEW are displayed here.

■ Server Information	OS	Server Status	DEW Key N...
☑ a 1 [redacted]	Linux	○ Running	KeyPair-5e22
□ a 1 [redacted] # Minor	Linux	○ Running	Install_Agent
□ a [redacted] # Minor	Linux	○ Running	Install_Agent

Step 10 In the row of a server, check its agent installation progress in the **Agent Status** column.

If the **Agent Status** is **Online**, the agent has been installed.

----End

Using a User-created Key to Install the Agent on One or Multiple Huawei Cloud Servers (Linux Only)

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

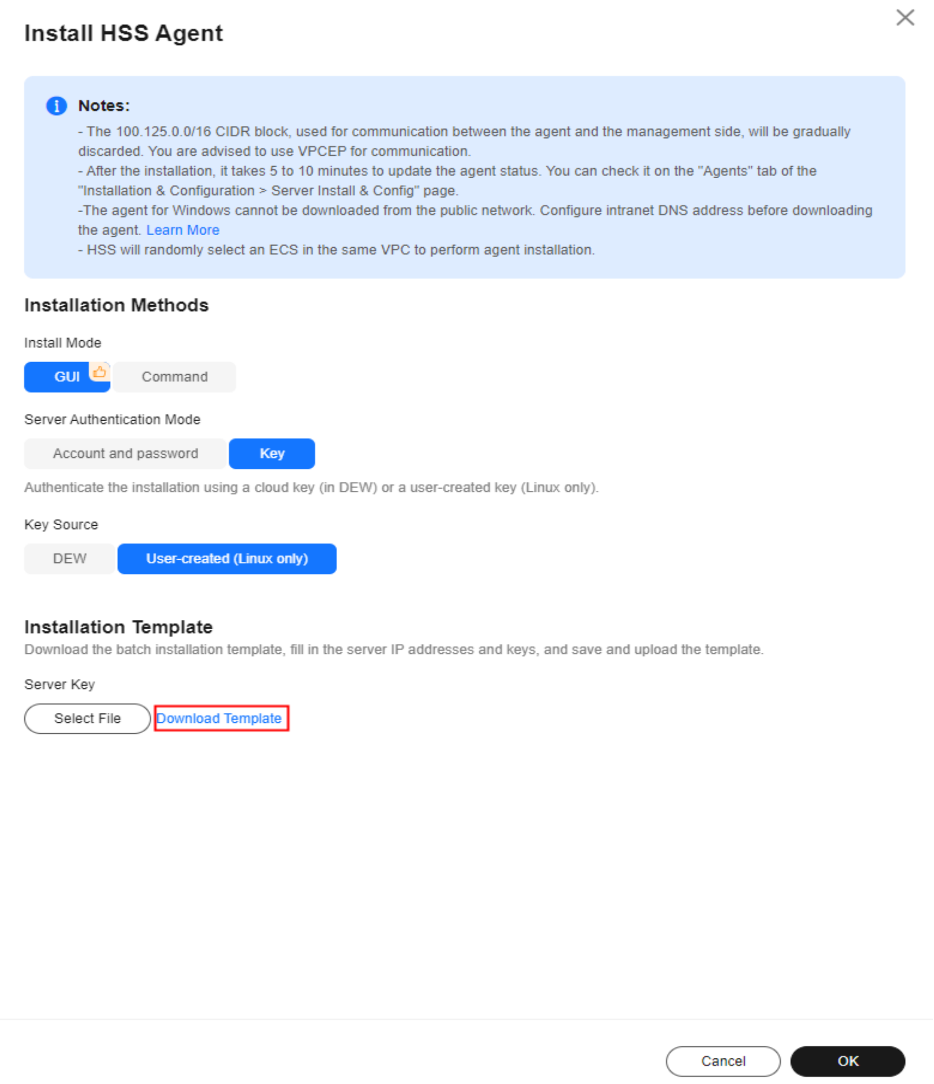
Step 8 Configure installation parameters as follows:

- **Install Mode**: Select **GUI**.
- **Server Authentication Mode**: Select **Key**.
- **Key Source**: Select **User-created key (Linux only)**.

Step 9 Upload the installation template.

1. Click **Download Template** to download the batch installation template to your local PC.

Figure 2-7 Downloading the batch installation template



Install HSS Agent

Notes:

- 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.
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Agents" tab of the "Installation & Configuration > Server Install & Config" page.
-The agent for Windows cannot be downloaded from the public network. Configure intranet DNS address before downloading the agent. Learn More
- HSS will randomly select an ECS in the same VPC to perform agent installation.

Installation Methods

Install Mode: GUI | Command

Server Authentication Mode: Account and password | Key

Authenticate the installation using a cloud key (in DEW) or a user-created key (Linux only).

Key Source: DEW | User-created (Linux only)

Installation Template

Download the batch installation template, fill in the server IP addresses and keys, and save and upload the template.

Server Key: Select File | Download Template

2. Open the downloaded file, fill in server information as required, and save the file.
3. Click **Select File** and upload the file.

   HSS will automatically parse the file and identify the servers you specified. If the parsing fails, you can click **View Failed Servers** and check the failure cause.

Step 10 Confirm the information and click **OK**.

Step 11 In the row of a server, check its agent installation progress in the **Agent Status** column.

If the **Agent Status** is **Online**, the agent has been installed.

----End

Using the Commands or Script to Install the Agent on Huawei Cloud Servers (Current-Account Installation)

The HSS agent can be installed using commands. You can install the agent on different OSs. Various installation methods are provided below.

Using Commands to Install the Agent on a Huawei Cloud Linux Server (Current-Account Installation)

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

Step 8 Configure installation parameters as follows:

- **Install Mode**: Select **Command**.
- **Owner Account**: Select **Current**.
- **Server OS**: Select **Linux**.
- **Scale**: Select **Single**.

Step 9 (Optional) Select the servers that need to be connected to the current HSS region and click **Next**.

- Perform this operation only in the **CN East2** and **CN Southwest-Guiyang1** regions. HSS will automatically create a VPC endpoint, which occupies an IP address of your VPC subnet. Only one VPC endpoint will be created for each of your VPCs to ensure the communication between your servers and HSS.

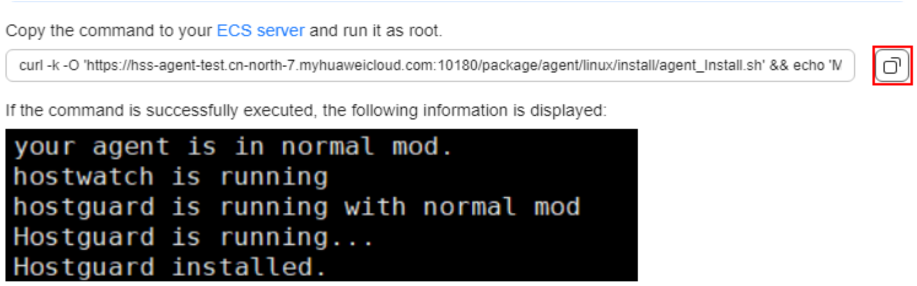
- In other regions, ensure the security groups of your servers allow outbound traffic through port 10180 of the 100.125.0.0/16 CIDR block. This port is used to communicate with HSS.

Step 10 Install the agent as prompted.

For **CN East2** and **CN Southwest-Guiyang1** regions, wait until the network communication succeeds (that is, the VPC endpoint is created) before performing the following operations.

1. On the console page, click ⧉ in the **Install HSS Agent** dialog box to copy the installation command.

Figure 2-8 Copying the installation command



Copy the command to your ECS server and run it as root.

```
curl -k -O 'https://hss-agent-test.cn-north-7.myhuaweicloud.com:10180/package/agent/linux/install/agent_Install.sh' && echo 'M
```

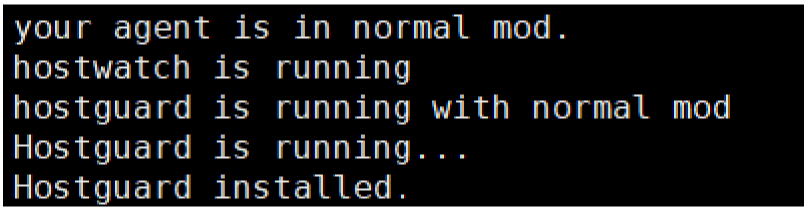
If the command is successfully executed, the following information is displayed:

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

2. Log in to the server as the **root** user and paste the installation command.

   If the command output shown in **Figure 2-9** is displayed, the agent has been installed.

Figure 2-9 Agent installed



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

3. Wait for 5 to 10 minutes and return to the HSS console. On the **Server Install & Config** page, click the **Agents** tab, and click **Servers with Agents**. Check the agent status of the target server.

   If the **Agent Status** is **Online**, the agent has been installed.

----End

Using Commands to Install the Agent on Multiple Huawei Cloud Linux Servers (Current-Account Installation)

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

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

Step 8 Configure installation parameters as follows:

- **Install Mode**: Select **Command**.
- **Owner Account**: Select **Current**.
- **Server OS**: Select **Linux**.
- **Scale**: Select **Batch**.
- **Server Authentication Mode**: Select **Account and password** or **Key** as needed.

Step 9 (Optional) Select the servers that need to be connected to the current HSS region and click **Next**.

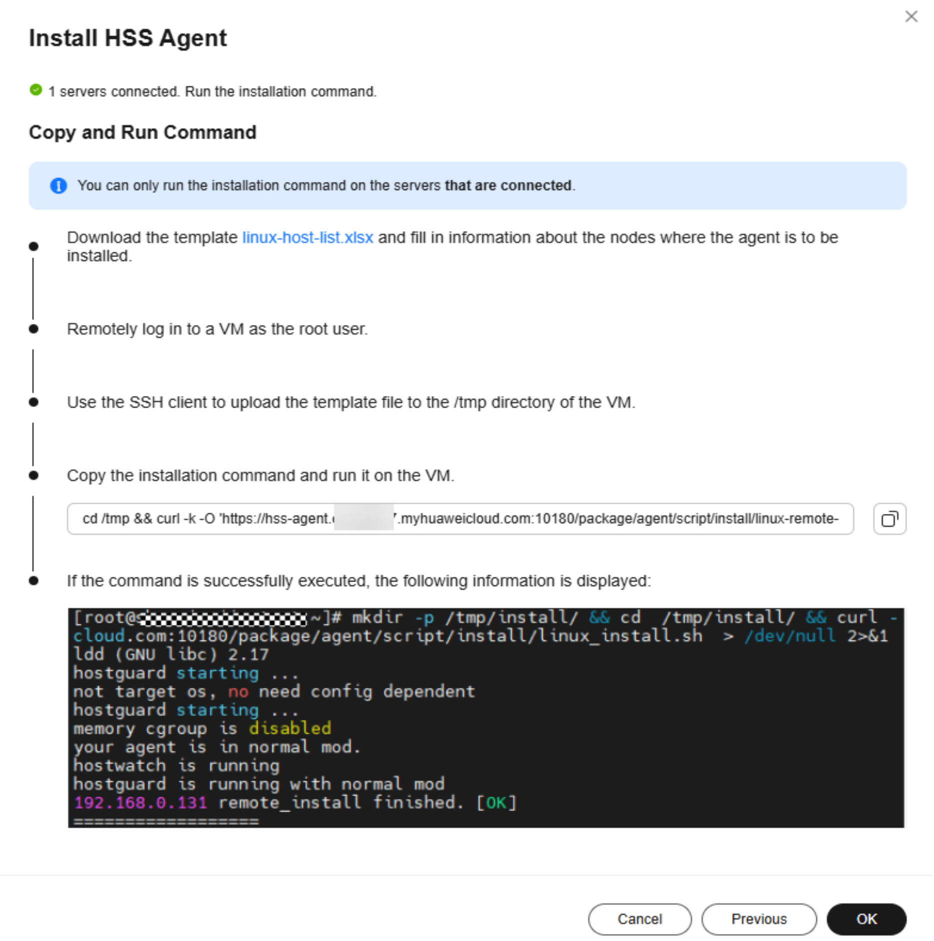
- Perform this operation only in the **CN East2** and **CN Southwest-Guiyang1** regions. HSS will automatically create a VPC endpoint, which occupies an IP address of your VPC subnet. Only one VPC endpoint will be created for each of your VPCs to ensure the communication between your servers and HSS.
- In other regions, ensure the security groups of your servers allow outbound traffic through port 10180 of the 100.125.0.0/16 CIDR block. This port is used to communicate with HSS.

Step 10 Install the agent as prompted.

For **CN East2** and **CN Southwest-Guiyang1** regions, wait until the network communication succeeds (that is, the VPC endpoint is created) before you proceed. Perform the following operations on any server:

1. On the console, click **linux-host-list.csv** in the **Install HSS Agent** dialog box to download the template.

Figure 2-10 Downloading linux-host-list.csv



1 servers connected. Run the installation command.

Copy and Run Command

You can only run the installation command on the servers **that are connected**.

- Download the template linux-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Remotely log in to a VM as the root user.
- Use the SSH client to upload the template file to the /tmp directory of the VM.
- Copy the installation command and run it on the VM.

```
cd /tmp && curl -k -O 'https://hss-agent.[redacted].myhuaweicloud.com:10180/package/agent/script/install/linux-remote-
```

- If the command is successfully executed, the following information is displayed:

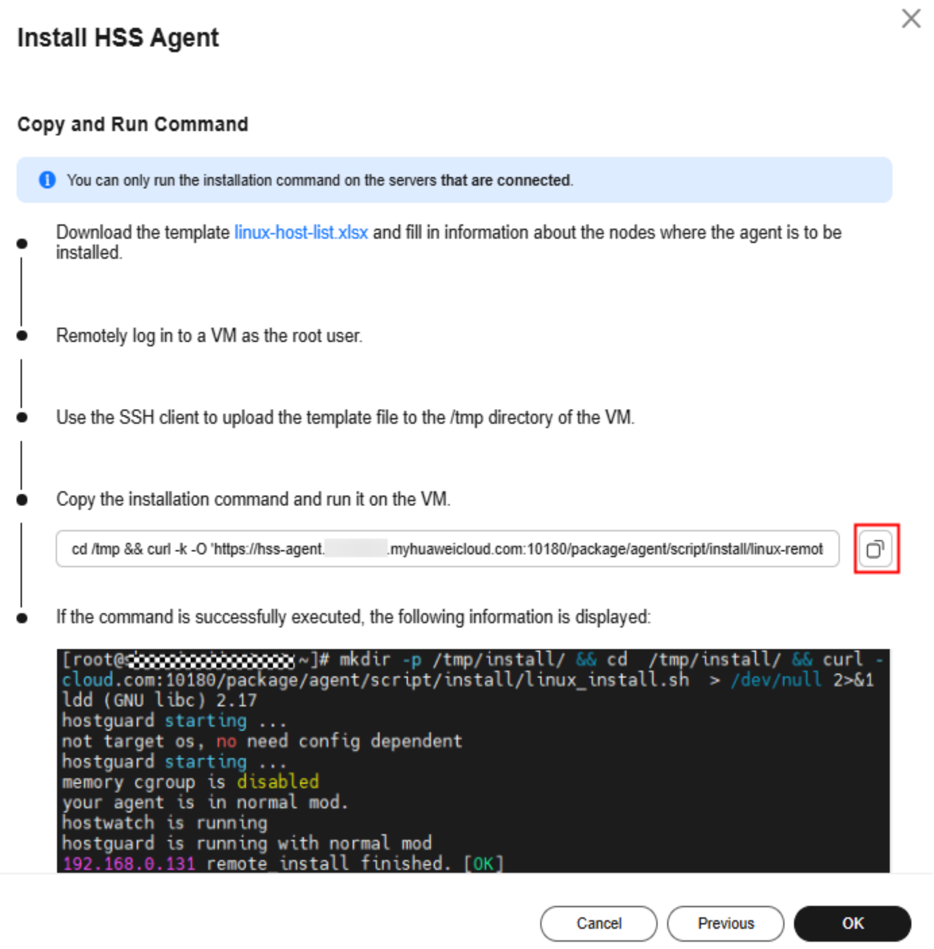
```
[root@s[redacted] ~]# mkdir -p /tmp/install/ && cd  /tmp/install/ && curl -
cloud.com:10180/package/agent/script/install/linux_install.sh  > /dev/null 2>&1
ldd (GNU libc) 2.17
hostguard starting ...
not target os, no need config dependent
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
192.168.0.131 remote_install finished. [OK]
==================
```

2. Enter the server information based on the requirements in the **linux-host-list.csv** template and save the template.

   Ensure that the entered server verification information is consistent with the verification mode selected in **Step 8**.

3. Use the **root** account to remotely log in to any target server.
4. Use the SSH client to upload the **linux-host-list.csv** file to the **/tmp** directory on the server.
5. Return to the HSS console. In the **Install HSS Agent** dialog box, click ⧉ to copy the installation command.

Figure 2-11 Copying the installation command



Copy and Run Command

You can only run the installation command on the servers that are connected.

- Download the template linux-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Remotely log in to a VM as the root user.
- Use the SSH client to upload the template file to the /tmp directory of the VM.
- Copy the installation command and run it on the VM.

```
cd /tmp && curl -k -O 'https://hss-agent.[redacted].myhuaweicloud.com:10180/package/agent/script/install/linux-remot
```

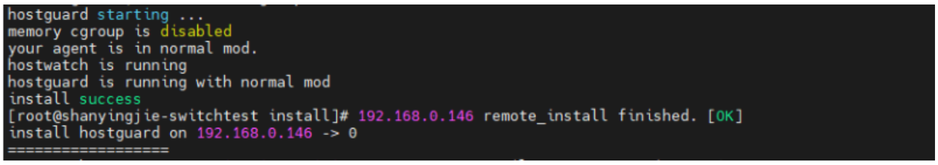
- If the command is successfully executed, the following information is displayed:

```
[root@[redacted]~]# mkdir -p /tmp/install/ && cd  /tmp/install/ && curl -
cloud.com:10180/package/agent/script/install/linux_install.sh  > /dev/null 2>&1
ldd (GNU libc) 2.17
hostguard starting ...
not target os, no need config dependent
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
192.168.0.131 remote_install finished. [OK]
```

6. Paste and run the installation command on the server to install the agent.

   If the information shown in **Figure 2-12** is displayed, the installation is complete.

Figure 2-12 Agent installed



```
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
install success
[root@shanyingjie-switchtest install]# 192.168.0.146 remote_install finished. [OK]
install hostguard on 192.168.0.146 -> 0
==================
```

7. Wait for 5 to 10 minutes and return to the HSS console. On the **Server Install & Config** page, click the **Agents** tab, and click **Servers with Agents**. Check the agent status of the target server.

   If the **Agent Status** is **Online**, the agent has been installed.

----End

Using the Script to Install the Agent on a Huawei Cloud Windows Server (Current-Account Installation)

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

Step 8 Configure installation parameters as follows:

- **Install Mode**: Select **Command**.
- **Owner Account**: Select **Current**.
- **Server OS**: Select **Windows**.
- **Scale**: Select **Single**.

Step 9 (Optional) Select the servers that need to be connected to the current HSS region and click **Next**.

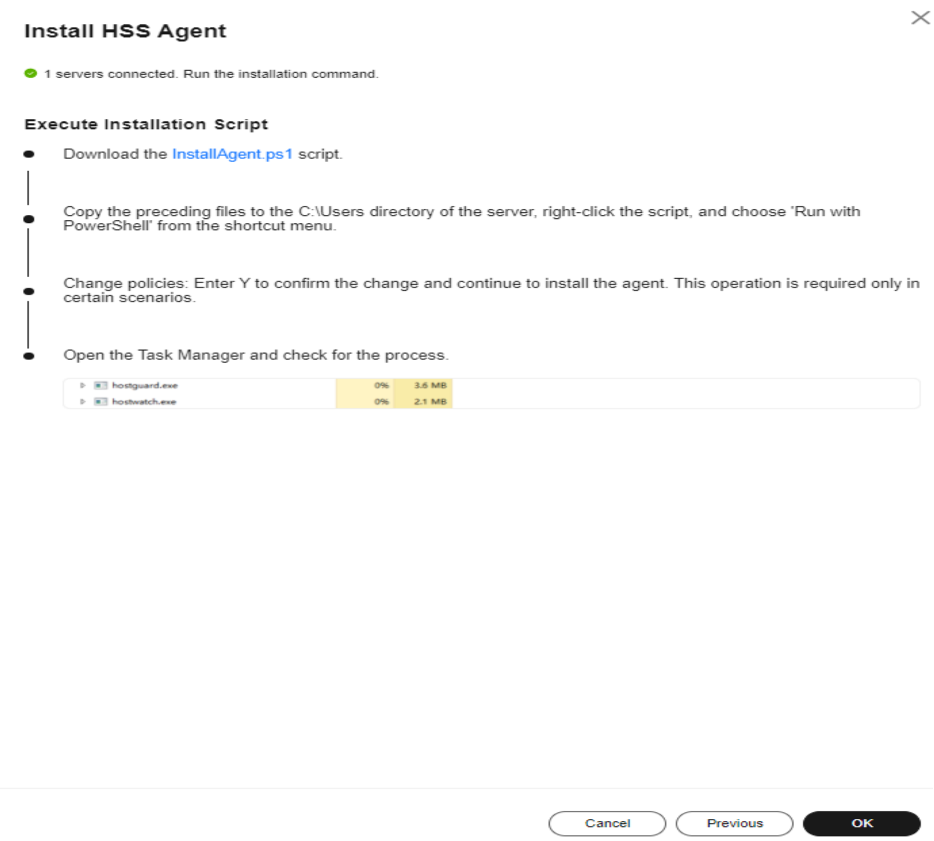
- Perform this operation only in the **CN East2** and **CN Southwest-Guiyang1** regions. HSS will automatically create a VPC endpoint, which occupies an IP address of your VPC subnet. Only one VPC endpoint will be created for each of your VPCs to ensure the communication between your servers and HSS.
- In other regions, ensure the security groups of your servers allow outbound traffic through port 10180 of the 100.125.0.0/16 CIDR block. This port is used to communicate with HSS.

Step 10 Install the agent as prompted.

For **CN East2** and **CN Southwest-Guiyang1** regions, wait until the network communication succeeds (that is, the VPC endpoint is created) before performing the following operations.

1. On the console, click **installAgent.ps1** in the **Install HSS Agent** dialog box to download the installation script.

Figure 2-13 Downloading installAgent.ps1



Install HSS Agent

1 servers connected. Run the installation command.

Execute Installation Script

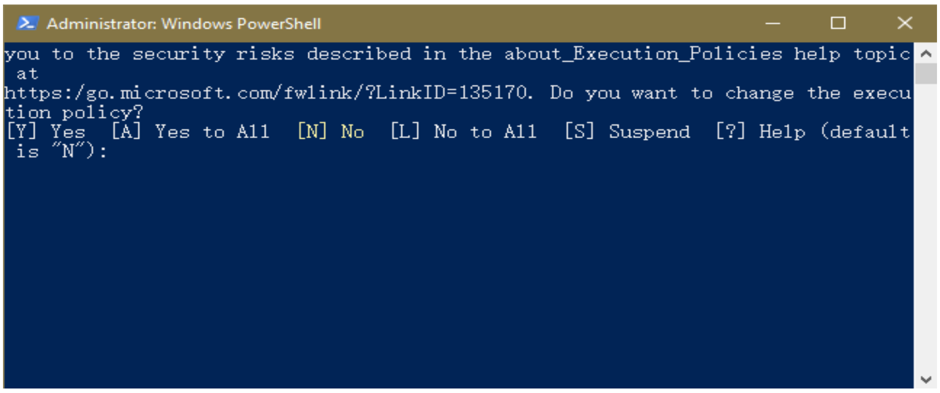
- Download the InstallAgent.ps1 script.
- Copy the preceding files to the C:\Users directory of the server, right-click the script, and choose 'Run with PowerShell' from the shortcut menu.
- Change policies: Enter Y to confirm the change and continue to install the agent. This operation is required only in certain scenarios.
- Open the Task Manager and check for the process.

hostguard.exe	0%	3.6 MB
hostwatch.exe	0%	2.1 MB

2. Copy the **installAgent.ps1** file to the **C:\Users** directory of the server where the agent is to be installed.
3. Right-click **installAgent.ps1** and choose **Run with PowerShell**.
4. (Optional) In the dialog box that is displayed, enter **Y** to run the script to install the agent.

   If no dialog box is displayed, skip this step.

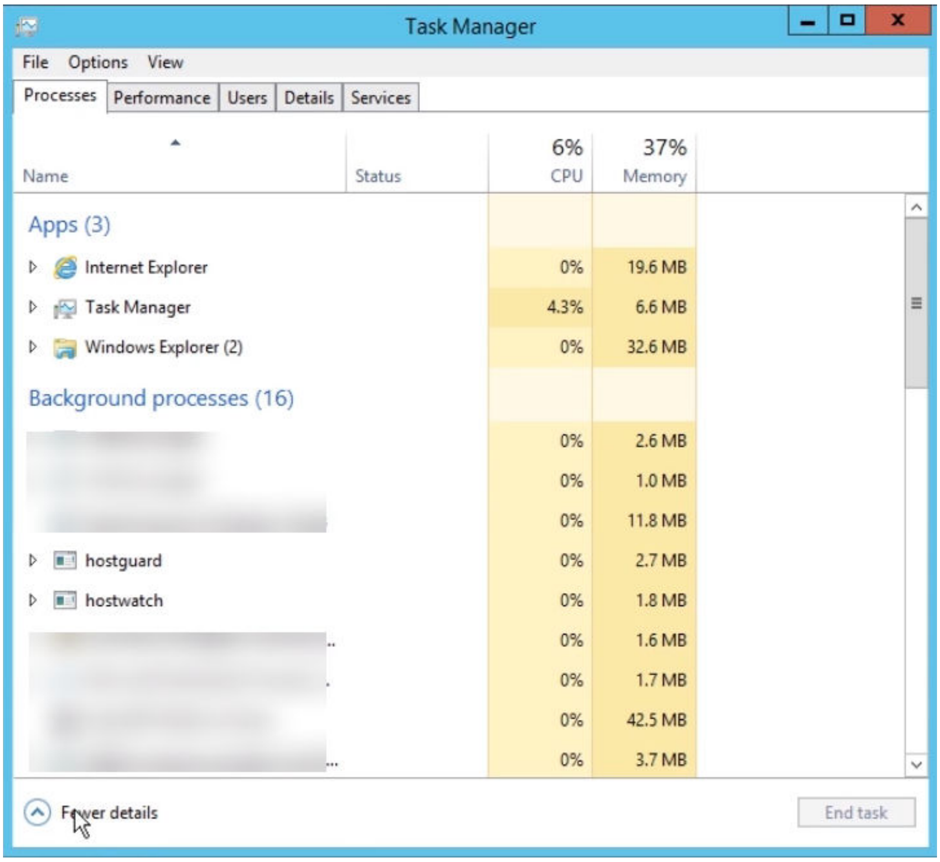
Figure 2-14 Changing the execution policy



```
you to the security risks described in the about_Execution_Policies help topic
 at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execu
tion policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default
 is "N"):
```

5. After the execution, open the Task Manager and check whether **hostguard.exe** and **hostwatch.exe** exist. If they do, the agent has been installed.

Figure 2-15 Agent installed



Name	Status	6% CPU	37% Memory
Apps (3)			
Internet Explorer		0%	19.6 MB
Task Manager		4.3%	6.6 MB
Windows Explorer (2)		0%	32.6 MB
Background processes (16)			
		0%	2.6 MB
		0%	1.0 MB
		0%	11.8 MB
hostguard		0%	2.7 MB
hostwatch		0%	1.8 MB
		0%	1.6 MB
		0%	1.7 MB
		0%	42.5 MB
		0%	3.7 MB

6. Wait for 5 to 10 minutes and return to the HSS console. On the **Server Install & Config** page, click the **Agents** tab, and click **Servers with Agents**. Check the agent status of the target server.

   If the **Agent Status** is **Online**, the agent has been installed.

----End

Using the Script to Install the Agent on Multiple Huawei Cloud Windows Servers (Current-Account Installation)

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

Step 8 Configure installation parameters as follows:

- **Install Mode**: Select **Command**.
- **Owner Account**: Select **Current**.
- **Server OS**: Select **Windows**.
- **Scale**: Select **Batch**.

Step 9 (Optional) Select the servers that need to be connected to the current HSS region and click **Next**.

- Perform this operation only in the **CN East2** and **CN Southwest-Guiyang1** regions. HSS will automatically create a VPC endpoint, which occupies an IP address of your VPC subnet. Only one VPC endpoint will be created for each of your VPCs to ensure the communication between your servers and HSS.
- In other regions, ensure the security groups of your servers allow outbound traffic through port 10180 of the 100.125.0.0/16 CIDR block. This port is used to communicate with HSS.

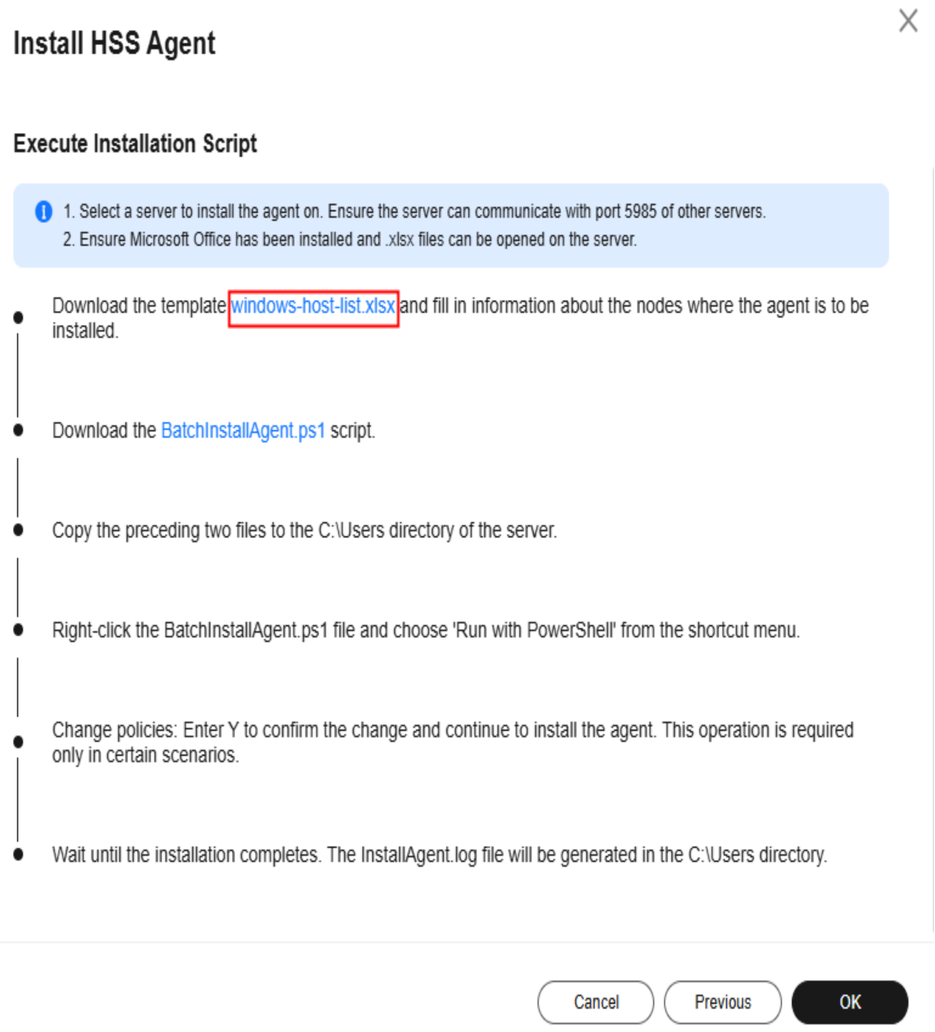
Step 10 Install the agent as prompted.

⚠ CAUTION

- For **CN East2** and **CN Southwest-Guiyang1** regions, wait until the network communication succeeds (that is, the VPC endpoint is created) before performing the following operations.
- Perform the following operations on any server.
- To install the agent, the server where the script is executed needs to access the port 5985 on other servers. Modify the inbound rules of the security groups on those servers to allow such access, or HSS will temporarily modify their security group rules while installing the agent. After the agent is installed, the modified settings will be deleted.

1. On the console, click **windows-host-list.xlsx** in the **Install HSS Agent** dialog box to download the template to the local PC.

Figure 2-16 Downloading windows-host-list.xlsx



Install HSS Agent

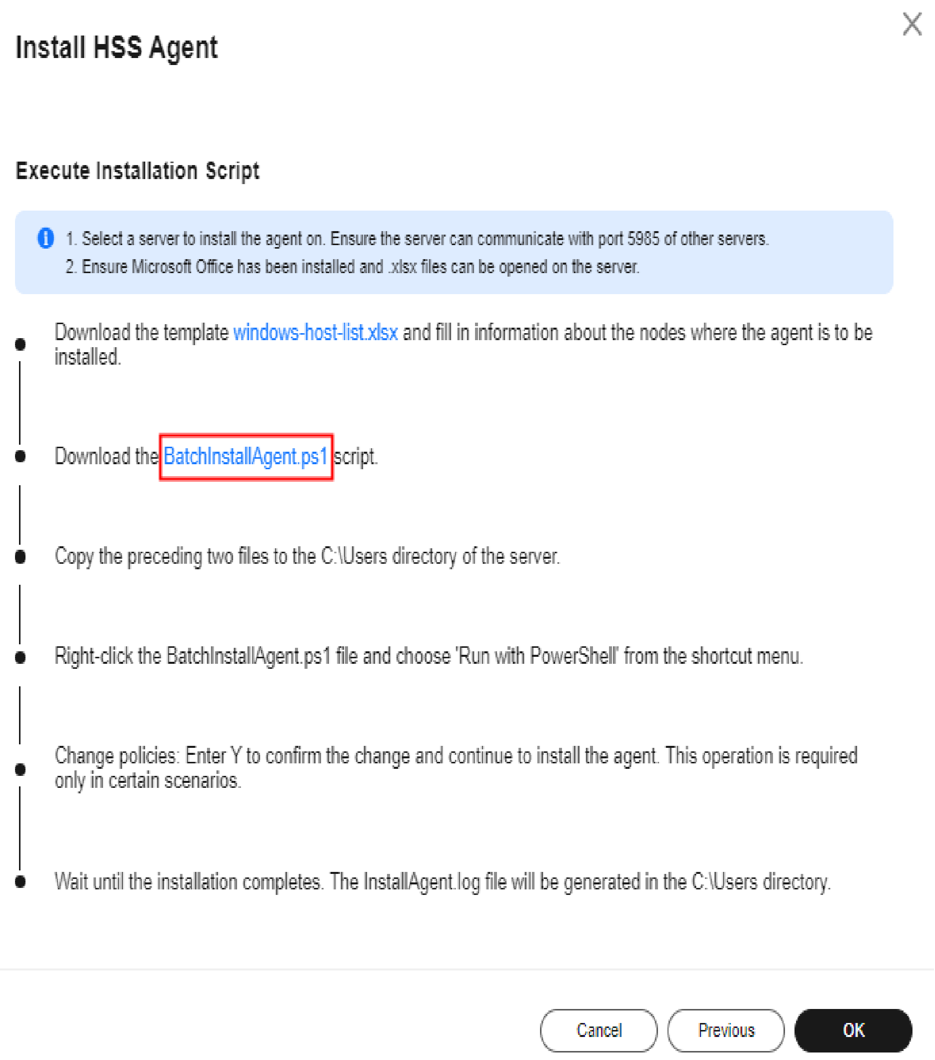
Execute Installation Script

1. Select a server to install the agent on. Ensure the server can communicate with port 5985 of other servers.
2. Ensure Microsoft Office has been installed and .xlsx files can be opened on the server.

- Download the template windows-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Download the BatchInstallAgent.ps1 script.
- Copy the preceding two files to the C:\Users directory of the server.
- Right-click the BatchInstallAgent.ps1 file and choose 'Run with PowerShell' from the shortcut menu.
- Change policies: Enter Y to confirm the change and continue to install the agent. This operation is required only in certain scenarios.
- Wait until the installation completes. The InstallAgent.log file will be generated in the C:\Users directory.

2. Enter server information based on the requirements in the **windows-host-list.xlsx** template and save it.
3. Return to the HSS console and click **BatchInstallAgent.ps1** to download the installation script.

Figure 2-17 Downloading BatchInstallAgent.ps1



Install HSS Agent

Execute Installation Script

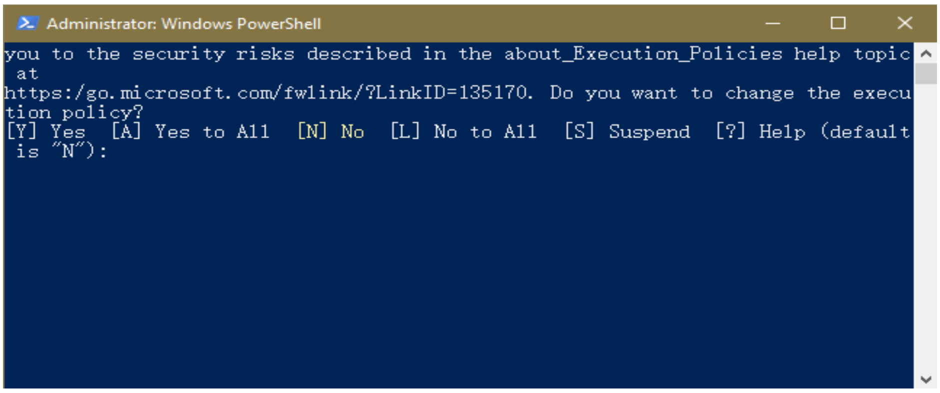
1. Select a server to install the agent on. Ensure the server can communicate with port 5985 of other servers.
2. Ensure Microsoft Office has been installed and .xlsx files can be opened on the server.

- Download the template windows-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Download the BatchInstallAgent.ps1 script.
- Copy the preceding two files to the C:\Users directory of the server.
- Right-click the BatchInstallAgent.ps1 file and choose 'Run with PowerShell' from the shortcut menu.
- Change policies: Enter Y to confirm the change and continue to install the agent. This operation is required only in certain scenarios.
- Wait until the installation completes. The InstallAgent.log file will be generated in the C:\Users directory.

4. Copy the **windows-host-list.xlsx** and **BatchInstallAgent.ps1** files to the **C:\Users** directory of the server where the agent is to be installed.
5. Right-click **BatchInstallAgent.ps1** and choose **Run with PowerShell**.
6. (Optional) In the dialog box that is displayed, enter **Y** to run the script to install the agent.

   If no dialog box is displayed, skip this step.

Figure 2-18 Changing the execution policy



```
you to the security risks described in the about_Execution_Policies help topic
 at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execu
tion policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default
 is "N"):
```

7. After the script is executed successfully, check whether the **BatchInstallAgent.log** file exists in **C:\Users\Administrator**.

   If the **BatchInstallAgent.log** file exists, the agent has been installed.

8. Wait for 5 to 10 minutes and return to the HSS console. On the **Server Install & Config** page, click the **Agents** tab, and click **Servers with Agents**. Check the agent status of the target server.

   If the **Agent Status** is **Online**, the agent has been installed.

----End

Using the Commands or Script to Install the Agent on Huawei Cloud Servers (Cross-Account Installation)

Assume you have two accounts. Account A is your management account. It needs to manage the servers under account B, a member account. You can log in to account A, copy the agent installation command or script, and run it on a server under account B. After the agent is installed, you can choose **Asset Management** > **Servers & Quota** under account A to view the servers and enable HSS for them. In this way, servers can be protected across accounts.

You can install the agent on different OSs. Various installation methods are as follows. The procedures assume you have account A (management account) and account B (its servers need to be managed by account A).

Using Commands to Install the Agent on a Huawei Cloud Linux Server (Cross-Account Installation)

Step 1 Log in to the management console using account A.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

Step 8 Select an installation mode and click **Next**.

- **Install Mode**: Select **Command**.
- **Owner Account**: Select **Other**.
- **Server OS**: Select **Linux**.
- **Scale**: Select **Single**.

Step 9 (Optional) Go to the VPCEP console and manually create a VPC endpoint for communication between the server and HSS.

Perform this operation only in the **CN East2** and **CN Southwest-Guiyang1** regions. Only one VPC endpoint needs to be created for each VPC. In other regions, ensure the security groups of your servers allow outbound traffic through port 10180 of the 100.125.0.0/16 CIDR block. This port is used to communicate with HSS.

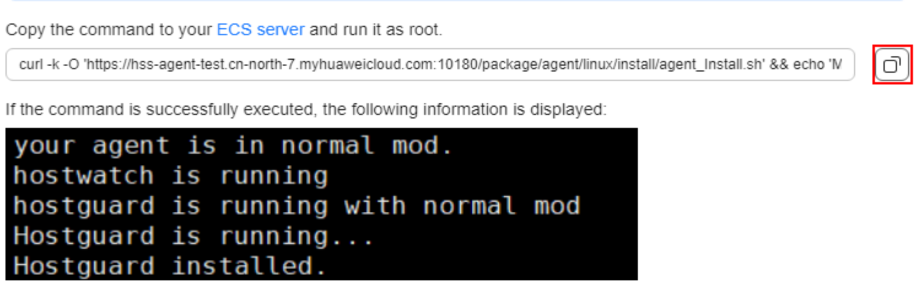
1. Click ☰ in the upper left corner of the page and choose **Networking** > **VPC Endpoint** to switch to the **VPC Endpoint** page.
2. In the upper right corner of the **VPC Endpoints** page, click **Buy VPC Endpoint**.
3. Set the parameters.
   a. **Region**: Select **CN East2** or **CN Southwest-Guiyang1**. Set the parameter based on the region to which the server is connected.
   b. **Service Category**: Select **Cloud service**.
   c. Selecting a service
      - Select **com.myhuaweicloud.xxx.hss-agent**. **xxx** indicates the region ID. For example, the region ID of CN East 2 is **cn-east-4**.
      - Select **Create a Private Domain Name**.

   d. **VPC**: Select a VPC that communicates with your server.
   e. **Subnet**: Select or create a subnet.
   f. **IPv4 Address**: Select **Automatically assign IP address**.
   g. Other parameters: Set parameters as prompted.
4. Click **Next** to submit the order.
5. Return to the **VPC Endpoints** page and confirm that the VPC endpoint is created.

Step 10 Return to the HSS console and install the agent as prompted.

1. On the console page, click ⧉ in the **Install HSS Agent** dialog box to copy the installation command.

Figure 2-19 Copying the installation command



Copy the command to your ECS server and run it as root.

```
curl -k -O 'https://hss-agent-test.cn-north-7.myhuaweicloud.com:10180/package/agent/linux/install/agent_Install.sh' && echo 'M
```

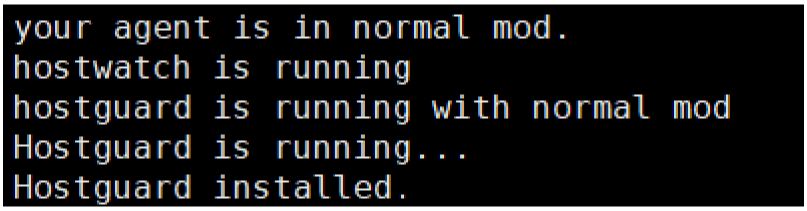
If the command is successfully executed, the following information is displayed:

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

2. Log in to the server under account B. Paste and run the installation command.

   If the command output shown in **Figure 2-20** is displayed, the agent has been installed.

Figure 2-20 Agent installed



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

3. Wait for 5 to 10 minutes. Return to the HSS console, choose **Asset Management** > **Servers & Quota**, and click the **Servers** tab. Check whether managed servers are online. If yes, the cross-account management is successful.

----End

Using Commands to Install the Agent on Multiple Huawei Cloud Linux Servers (Cross-Account Installation)

Step 1 **Log in to the management console** using account A.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

Step 8 Select an installation mode and click **Next**.

- **Install Mode**: Select **Command**.
- **Owner Account**: Select **Other**.

- **Server OS**: Select **Linux**.
- **Scale**: Select **Batch**.
- **Server Authentication Mode**: Select **Account and password** or **Key** as needed.

Step 9 (Optional) Go to the VPCEP console and manually create a VPC endpoint for communication between the server and HSS.

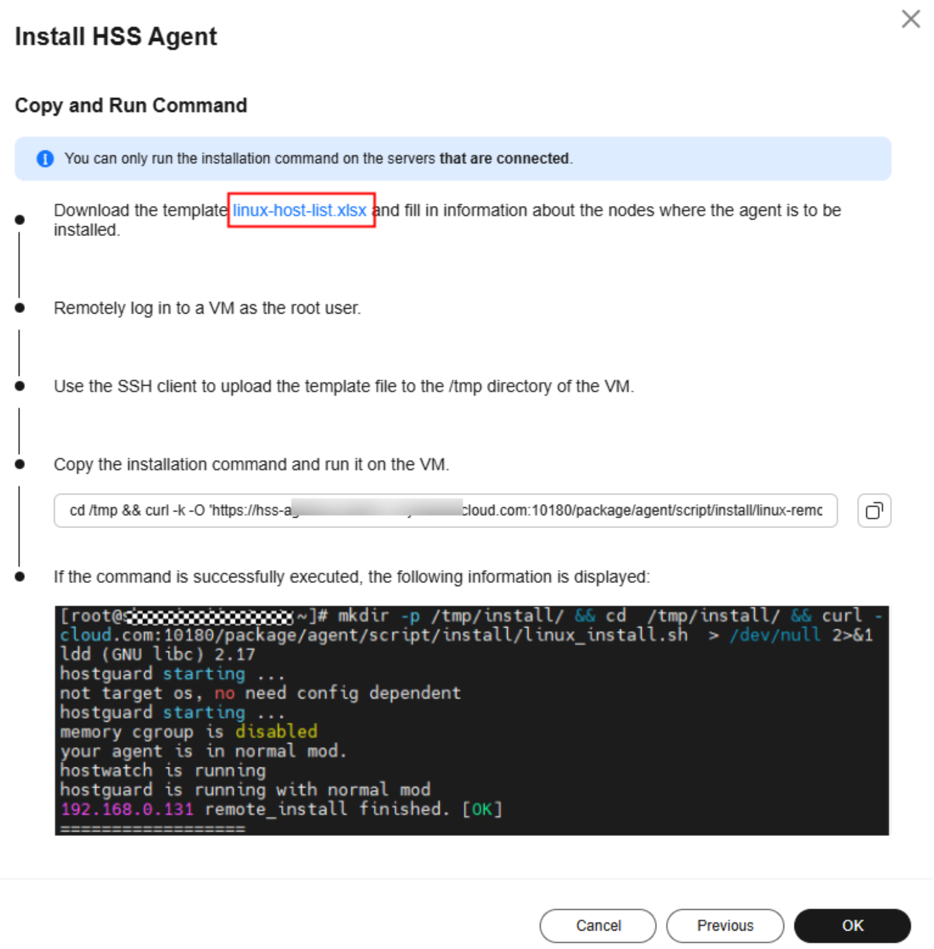
Perform this operation only in the **CN East2** and **CN Southwest-Guiyang1** regions. Only one VPC endpoint needs to be created for each VPC. In other regions, ensure the security groups of your servers allow outbound traffic through port 10180 of the 100.125.0.0/16 CIDR block. This port is used to communicate with HSS.

1. Click ☰ in the upper left corner of the page and choose **Networking** > **VPC Endpoint** to switch to the **VPC Endpoint** page.
2. In the upper right corner of the **VPC Endpoints** page, click **Buy VPC Endpoint**.
3. Set the parameters.
   a. **Region**: Select **CN East2** or **CN Southwest-Guiyang1**. Set the parameter based on the region to which the server is connected.
   b. **Service Category**: Select **Cloud service**.
   c. Selecting a service
      - Select **com.myhuaweicloud.xxx.hss-agent**. **xxx** indicates the region ID. For example, the region ID of CN East 2 is **cn-east-4**.
      - Select **Create a Private Domain Name**.
   d. **VPC**: Select a VPC that communicates with your server.
   e. **Subnet**: Select or create a subnet.
   f. **IPv4 Address**: Select **Automatically assign IP address**.
   g. Other parameters: Set parameters as prompted.
4. Click **Next** to submit the order.
5. Return to the **VPC Endpoints** page and confirm that the VPC endpoint is created.

Step 10 Return to the HSS console and install the agent as prompted.

1. On the console, click **linux-host-list.csv** in the **Install HSS Agent** dialog box to download the template.

Figure 2-21 Downloading linux-host-list.csv



Install HSS Agent

Copy and Run Command

You can only run the installation command on the servers **that are connected**.

- Download the template linux-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Remotely log in to a VM as the root user.
- Use the SSH client to upload the template file to the /tmp directory of the VM.
- Copy the installation command and run it on the VM.

```
cd /tmp && curl -k -O 'https://hss-a[redacted]cloud.com:10180/package/agent/script/install/linux-remc
```

- If the command is successfully executed, the following information is displayed:

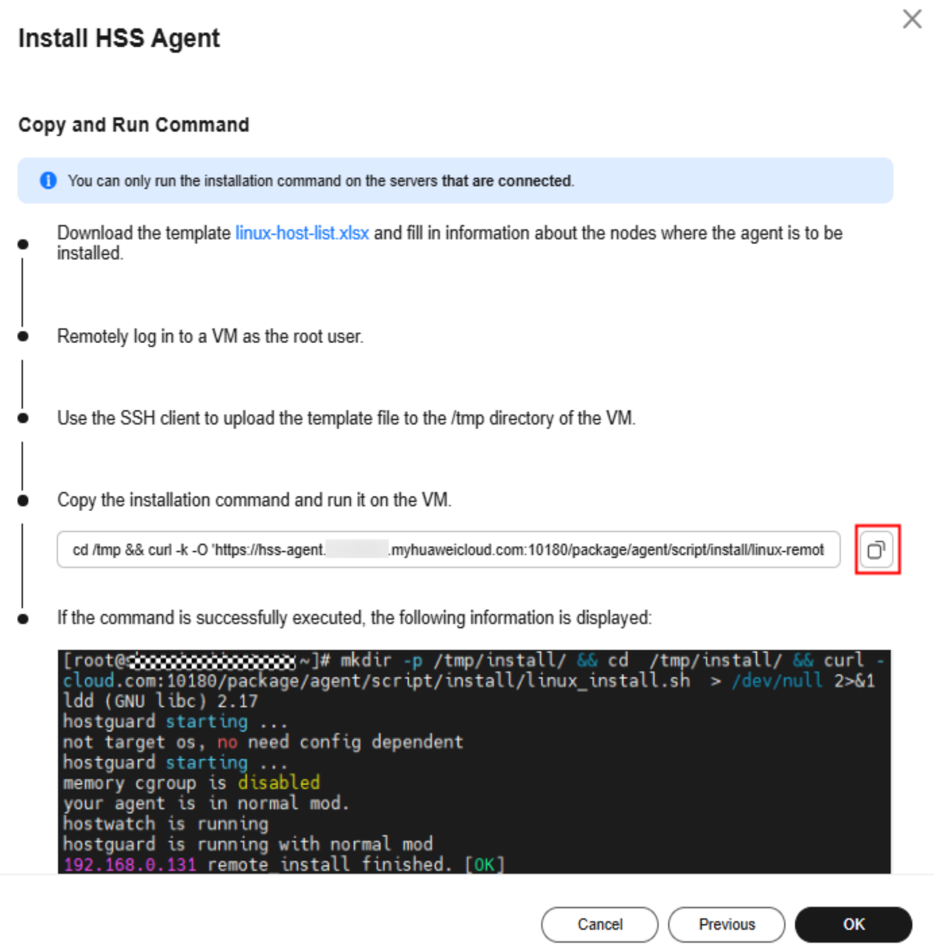
```
[root@s[redacted]~]# mkdir -p /tmp/install/ && cd  /tmp/install/ && curl -
cloud.com:10180/package/agent/script/install/linux_install.sh  > /dev/null 2>&1
ldd (GNU libc) 2.17
hostguard starting ...
not target os, no need config dependent
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
192.168.0.131 remote_install finished. [OK]
==================
```

2. In the **linux-host-list.csv** template, fill in the information about account B's servers that need to be managed, and save the information.

   Ensure that the entered server verification information is consistent with the verification mode selected in **Step 8**.

3. Use the **root** account to remotely log in to any of account B's servers that need to be managed.
4. Use the SSH client to upload the **linux-host-list.csv** file to the **/tmp** directory on the server.
5. Return to the HSS console. In the **Install HSS Agent** dialog box, click ⧉ to copy the installation command.

Figure 2-22 Copying the installation command



Install HSS Agent

Copy and Run Command

You can only run the installation command on the servers that are connected.

- Download the template linux-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Remotely log in to a VM as the root user.
- Use the SSH client to upload the template file to the /tmp directory of the VM.
- Copy the installation command and run it on the VM.

```
cd /tmp && curl -k -O 'https://hss-agent.[redacted].myhuaweicloud.com:10180/package/agent/script/install/linux-remot
```

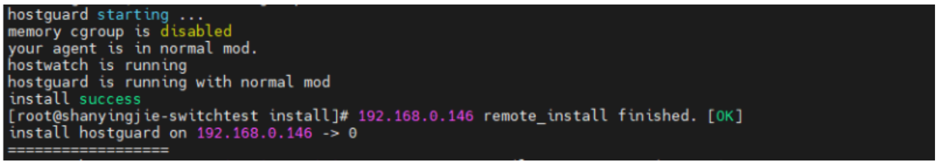
- If the command is successfully executed, the following information is displayed:

```
[root@[redacted]~]# mkdir -p /tmp/install/ && cd  /tmp/install/ && curl -
cloud.com:10180/package/agent/script/install/linux_install.sh  > /dev/null 2>&1
ldd (GNU libc) 2.17
hostguard starting ...
not target os, no need config dependent
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
192.168.0.131 remote install finished. [OK]
```

6. Paste and run the installation command on the server to install the agent.

   If the information shown in **Figure 2-23** is displayed, the installation is complete.

Figure 2-23 Agent installed



```
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
install success
[root@shanyingjie-switchtest install]# 192.168.0.146 remote_install finished. [OK]
install hostguard on 192.168.0.146 -> 0
==================
```

7. Wait for 5 to 10 minutes. Return to the HSS console, choose **Asset Management** > **Servers & Quota**, and click the **Servers** tab. Check whether managed servers are online. If yes, the cross-account management is successful.

----End

Using the Script to Install the Agent on a Huawei Cloud Windows Server (Cross-Account Installation)

Step 1 Log in to the management console using account A.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

Step 8 Select an installation mode and click **Next**.

- **Install Mode**: Select **Command**.
- **Owner Account**: Select **Other**.
- **Server OS**: Select **Windows**.
- **Scale**: Select **Single**.

Step 9 (Optional) Go to the VPCEP console and manually create a VPC endpoint for communication between the server and HSS.

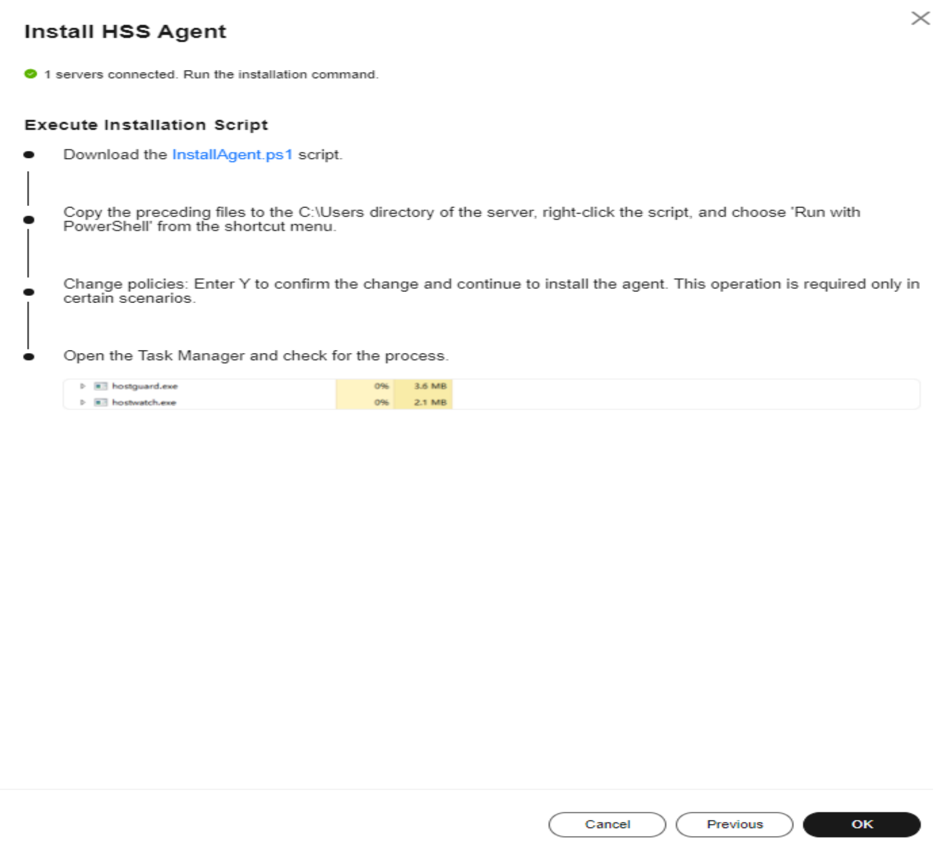
Perform this operation only in the **CN East2** and **CN Southwest-Guiyang1** regions. Only one VPC endpoint needs to be created for each VPC. In other regions, ensure the security groups of your servers allow outbound traffic through port 10180 of the 100.125.0.0/16 CIDR block. This port is used to communicate with HSS.

1. Click ☰ in the upper left corner of the page and choose **Networking** > **VPC Endpoint** to switch to the **VPC Endpoint** page.
2. In the upper right corner of the **VPC Endpoints** page, click **Buy VPC Endpoint**.
3. Set the parameters.
   a. **Region**: Select **CN East2** or **CN Southwest-Guiyang1**. Set the parameter based on the region to which the server is connected.
   b. **Service Category**: Select **Cloud service**.
   c. Selecting a service
      - Select **com.myhuaweicloud.xxx.hss-agent**. **xxx** indicates the region ID. For example, the region ID of CN East 2 is **cn-east-4**.
      - Select **Create a Private Domain Name**.
   d. **VPC**: Select a VPC that communicates with your server.
   e. **Subnet**: Select or create a subnet.
   f. **IPv4 Address**: Select **Automatically assign IP address**.
   g. Other parameters: Set parameters as prompted.
4. Click **Next** to submit the order.
5. Return to the **VPC Endpoints** page and confirm that the VPC endpoint is created.

Step 10 Return to the HSS console and install the agent as prompted.

1. On the console, click **installAgent.ps1** in the **Install HSS Agent** dialog box to download the installation script.

Figure 2-24 Downloading installAgent.ps1



Install HSS Agent

1 servers connected. Run the installation command.

Execute Installation Script

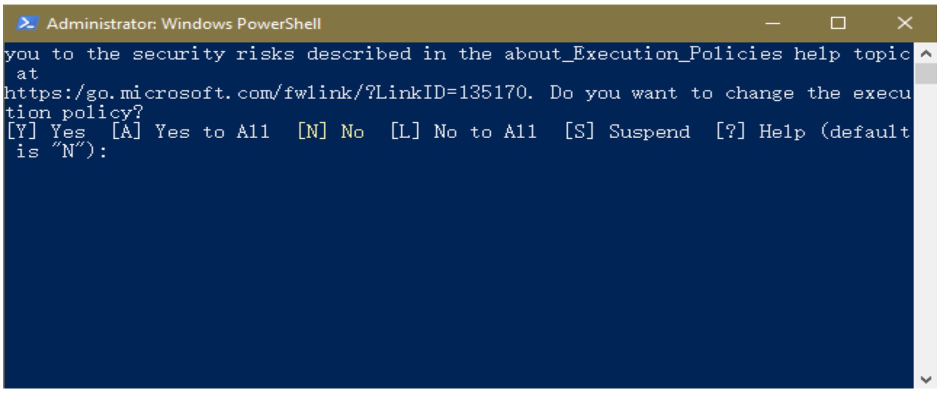
- Download the InstallAgent.ps1 script.
- Copy the preceding files to the C:\Users directory of the server, right-click the script, and choose 'Run with PowerShell' from the shortcut menu.
- Change policies: Enter Y to confirm the change and continue to install the agent. This operation is required only in certain scenarios.
- Open the Task Manager and check for the process.

hostguard.exe	0%	3.6 MB
hostwatch.exe	0%	2.1 MB

2. Copy the **installAgent.ps1** file to the **C:\Users** directory of the server under account B.
3. Right-click **installAgent.ps1** and choose **Run with PowerShell**.
4. (Optional) In the dialog box that is displayed, enter **Y** to run the script to install the agent.

   If no dialog box is displayed, skip this step.

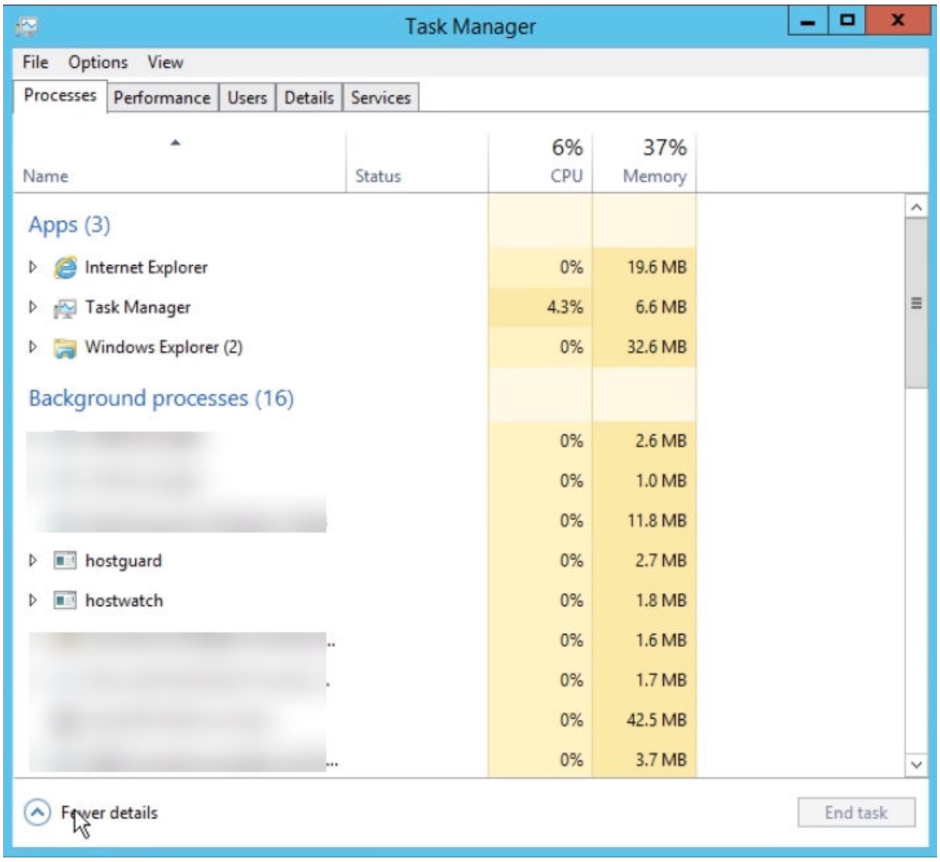
Figure 2-25 Changing the execution policy



```
you to the security risks described in the about_Execution_Policies help topic
 at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execu
tion policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default
 is "N"):
```

5. After the execution, open the Task Manager and check whether **hostguard.exe** and **hostwatch.exe** exist. If they do, the agent has been installed.

Figure 2-26 Agent installed



Name	Status	6% CPU	37% Memory
Apps (3)			
Internet Explorer		0%	19.6 MB
Task Manager		4.3%	6.6 MB
Windows Explorer (2)		0%	32.6 MB
Background processes (16)			
[redacted]		0%	2.6 MB
[redacted]		0%	1.0 MB
[redacted]		0%	11.8 MB
hostguard		0%	2.7 MB
hostwatch		0%	1.8 MB
[redacted]		0%	1.6 MB
[redacted]		0%	1.7 MB
[redacted]		0%	42.5 MB
[redacted]		0%	3.7 MB

6. Wait for 5 to 10 minutes. Return to the HSS console, choose **Asset Management** > **Servers & Quota**, and click the **Servers** tab. Check whether managed servers are online. If yes, the cross-account management is successful.

----End

Using the Script to Install the Agent on Multiple Huawei Cloud Windows Servers (Cross-Account Installation)

Step 1 Log in to the management console using account A.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **ECS** and click **Configure Now**.

Step 8 Select an installation mode and click **Next**.

- **Install Mode**: Select **Command**.
- **Owner Account**: Select **Other**.
- **Server OS**: Select **Windows**.
- **Scale**: Select **Batch**.

Step 9 (Optional) Go to the VPCEP console and manually create a VPC endpoint for communication between the server and HSS.

Perform this operation only in the **CN East2** and **CN Southwest-Guiyang1** regions. Only one VPC endpoint needs to be created for each VPC. In other regions, ensure the security groups of your servers allow outbound traffic through port 10180 of the 100.125.0.0/16 CIDR block. This port is used to communicate with HSS.

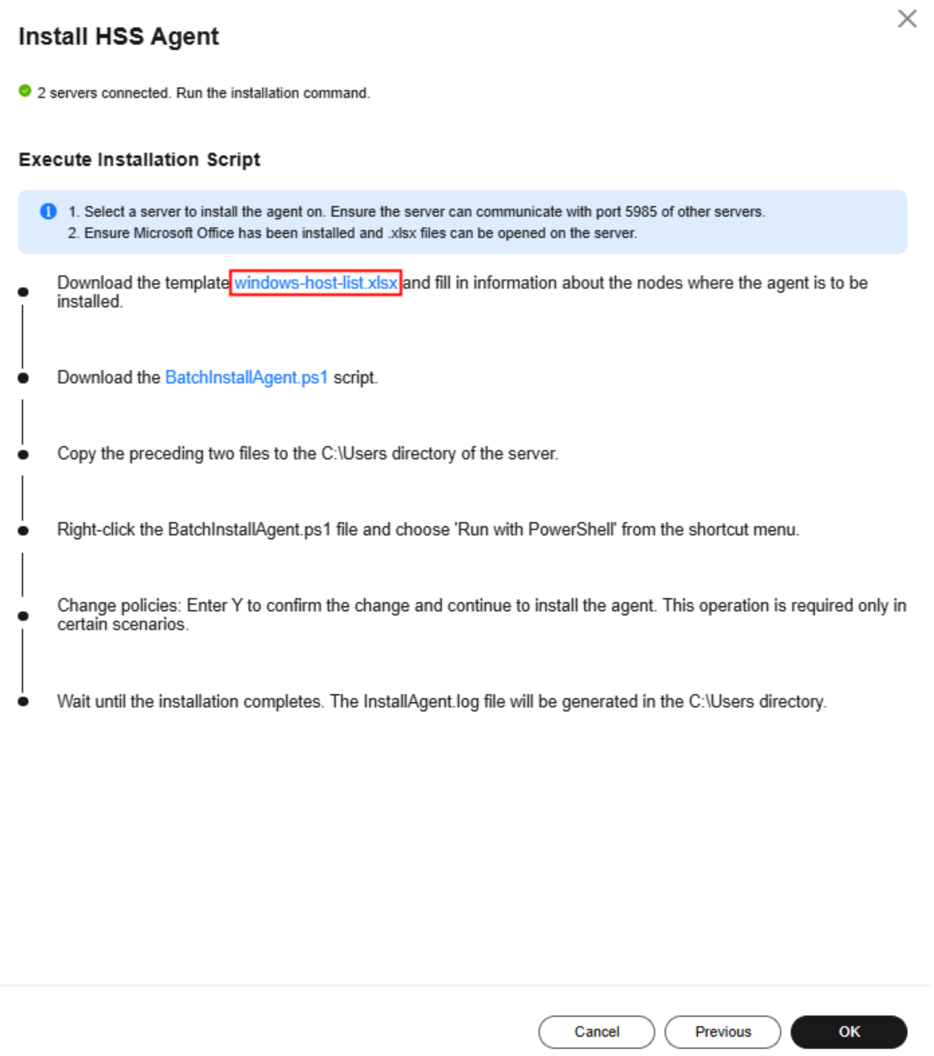
1. Click ☰ in the upper left corner of the page and choose **Networking** > **VPC Endpoint** to switch to the **VPC Endpoint** page.
2. In the upper right corner of the **VPC Endpoints** page, click **Buy VPC Endpoint**.
3. Set the parameters.
    a. **Region**: Select **CN East2** or **CN Southwest-Guiyang1**. Set the parameter based on the region to which the server is connected.
    b. **Service Category**: Select **Cloud service**.
    c. Selecting a service
        - Select **com.myhuaweicloud.xxx.hss-agent**. **xxx** indicates the region ID. For example, the region ID of CN East 2 is **cn-east-4**.
        - Select **Create a Private Domain Name**.
    d. **VPC**: Select a VPC that communicates with your server.
    e. **Subnet**: Select or create a subnet.
    f. **IPv4 Address**: Select **Automatically assign IP address**.
    g. Other parameters: Set parameters as prompted.
4. Click **Next** to submit the order.
5. Return to the **VPC Endpoints** page and confirm that the VPC endpoint is created.

Step 10 Return to the HSS console and install the agent as prompted.

Perform this operation only in the **CN East2** and **CN Southwest-Guiyang1** regions. Only one VPC endpoint needs to be created for each VPC. In other regions, ensure the security groups of your servers allow outbound traffic through port 10180 of the 100.125.0.0/16 CIDR block. This port is used to communicate with HSS.

1. On the console, click **windows-host-list.xlsx** in the **Install HSS Agent** dialog box to download the template to the local PC.

Figure 2-27 Downloading windows-host-list.xlsx



Install HSS Agent

2 servers connected. Run the installation command.

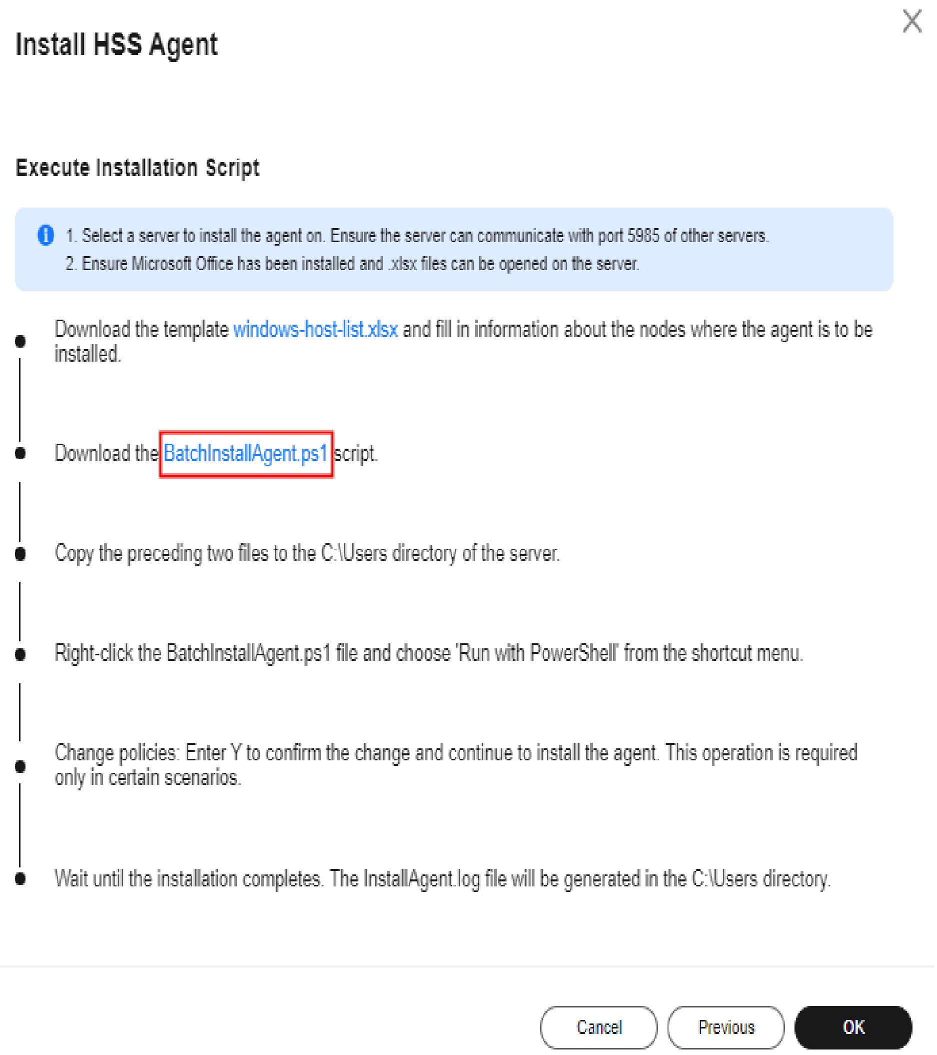
Execute Installation Script

1. Select a server to install the agent on. Ensure the server can communicate with port 5985 of other servers.
2. Ensure Microsoft Office has been installed and .xlsx files can be opened on the server.

- Download the template windows-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Download the BatchInstallAgent.ps1 script.
- Copy the preceding two files to the C:\Users directory of the server.
- Right-click the BatchInstallAgent.ps1 file and choose 'Run with PowerShell' from the shortcut menu.
- Change policies: Enter Y to confirm the change and continue to install the agent. This operation is required only in certain scenarios.
- Wait until the installation completes. The InstallAgent.log file will be generated in the C:\Users directory.

2. In the **windows-host-list.xlsx** template, fill in the information about account B's servers that need to be managed, and save the information.
3. Return to the HSS console and click **BatchInstallAgent.ps1** to download the installation script.

Figure 2-28 Downloading BatchInstallAgent.ps1



Install HSS Agent

Execute Installation Script

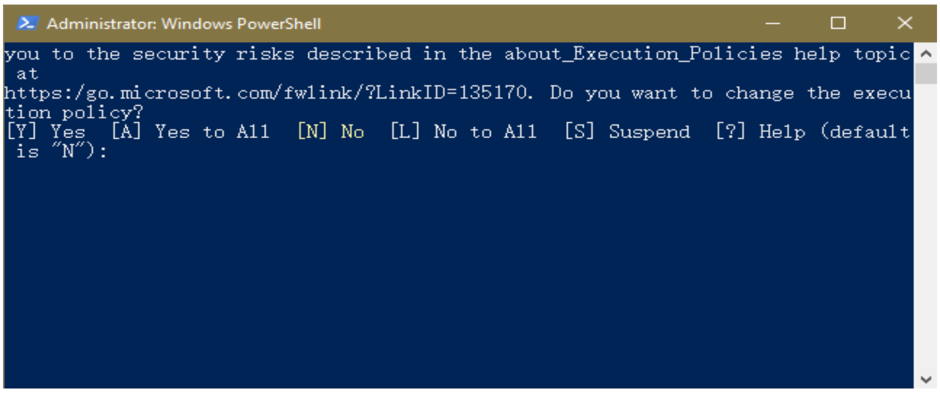
1. Select a server to install the agent on. Ensure the server can communicate with port 5985 of other servers.
2. Ensure Microsoft Office has been installed and .xlsx files can be opened on the server.

- Download the template windows-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Download the BatchInstallAgent.ps1 script.
- Copy the preceding two files to the C:\Users directory of the server.
- Right-click the BatchInstallAgent.ps1 file and choose 'Run with PowerShell' from the shortcut menu.
- Change policies: Enter Y to confirm the change and continue to install the agent. This operation is required only in certain scenarios.
- Wait until the installation completes. The InstallAgent.log file will be generated in the C:\Users directory.

4. Copy and paste the **windows-host-list.xlsx** and **BatchInstallAgent.ps1** files to the **C:\Users** directory on any of account B's servers to be managed.
5. Right-click **BatchInstallAgent.ps1** and choose **Run with PowerShell**.
6. (Optional) In the dialog box that is displayed, enter **Y** to run the script to install the agent.

   If no dialog box is displayed, skip this step.

Figure 2-29 Changing the execution policy



```
you to the security risks described in the about_Execution_Policies help topic
 at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execu
tion policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default
 is "N"):
```

7. After the script is executed successfully, check whether the **BatchInstallAgent.log** file exists in **C:\Users\Administrator**.

   If the **BatchInstallAgent.log** file exists, the agent has been installed.

8. Wait for 5 to 10 minutes. Return to the HSS console, choose **Asset Management** > **Servers & Quota**, and click the **Servers** tab. Check whether managed servers are online. If yes, the cross-account management is successful.

----End

FAQ

For details about how to troubleshoot the agent installation failure, see **What Should I Do If Agent Installation Failed?**

Follow-up Procedure

After the agent is installed on the server or container node, **enable protection**.

2.3.4 Installing the Agent on Third-party Servers

Scenario

You can enable HSS for servers only after installing the agent. For third-party cloud servers and on-premises data centers (IDCs) that can access the Internet, you can download and install the HSS agent through the Internet and connect the servers to the HSS console for protection management.

This section describes how to install the agent on a third-party server through the Internet.

Prerequisites

Perform the operations in **Checking the Installation Environment** to ensure agent installation is not affected by DNS server addresses, third-party security software, or the outbound port settings of security groups.

Constraints

- Third-party cloud servers and on-premises IDC can be connected to HSS through the Internet in the following regions: **CN North-Beijing1**, **CN North-Beijing4**, **CN East-Shanghai1**, **CN East-Shanghai2**, **CN South-Guangzhou**, **CN Southwest-Guiyang1**, **CN-Hong Kong**, **AP-Singapore**, **AP-Jakarta**, and **ME-Riyadh**.
- If your server cannot access the Internet and needs to be connected to HSS for protection, refer to the following solutions:
  - For **CN East2** and **Southwest-Guiyang1** regions: **Connecting Third-party Servers to HSS Through Direct Connect and VPC Endpoints**
  - For regions other than **CN East2** and **Southwest-Guiyang1**: **Third-Party Servers Accessing HSS Through Direct Connect and Proxy Servers**.

Installing the Agent on Third-party Linux Servers Using Commands

The following describes how to install the agent on the Linux server. You can select a method as required.

Installing the Agent on a Single Third-party Linux Server Using Commands

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

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

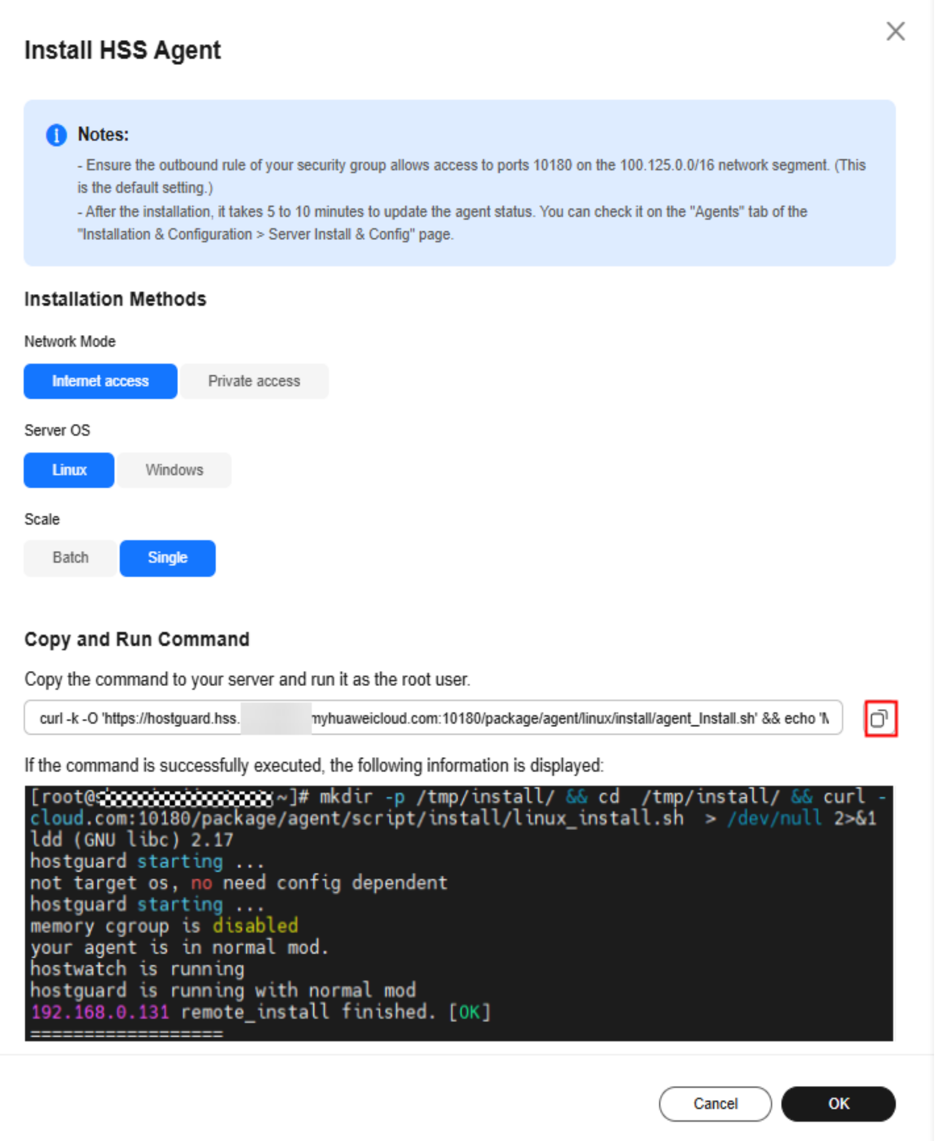
Step 7 Select **Third-party Cloud or Data Center Server** and click **Configure Now**.

Step 8 Select an installation method.

- **Network Mode**: **Internet access**
- **Server OS**: **Linux**
- **Scale**: **Single**

Step 9 Click ⧉ to copy the installation command.

Figure 2-30 Copying the installation command



Install HSS Agent

Notes:
- Ensure the outbound rule of your security group allows access to ports 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Agents" tab of the "Installation & Configuration > Server Install & Config" page.

Installation Methods

Network Mode: [✓ Internet access] Private access

Server OS: [✓ Linux] Windows

Scale: Batch [✓ Single]

Copy and Run Command

Copy the command to your server and run it as the root user.

```
curl -k -O 'https://hostguard.hss.[redacted]myhuaweicloud.com:10180/package/agent/linux/install/agent_Install.sh' && echo 'N
```

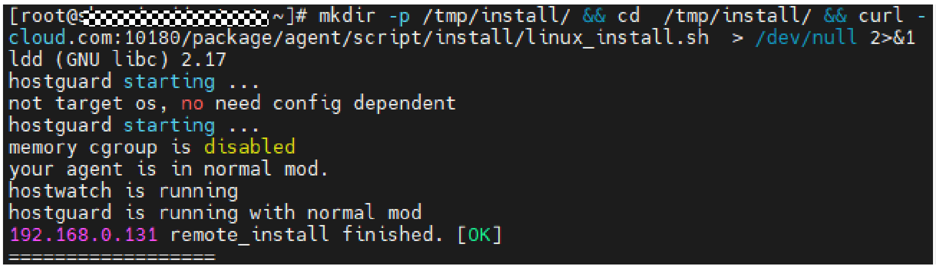
If the command is successfully executed, the following information is displayed:

```
[root@[redacted]~]# mkdir -p /tmp/install/ && cd  /tmp/install/ && curl -
cloud.com:10180/package/agent/script/install/linux_install.sh  > /dev/null 2>&1
ldd (GNU libc) 2.17
hostguard starting ...
not target os, no need config dependent
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
192.168.0.131 remote_install finished. [OK]
==================
```

Step 10 Log in to the server as user **root**, and paste and run the installation command.

If the command output shown in **Figure 2-31** is displayed, the agent has been installed.

Figure 2-31 Agent installed



```
[root@[redacted]~]# mkdir -p /tmp/install/ && cd  /tmp/install/ && curl -
cloud.com:10180/package/agent/script/install/linux_install.sh  > /dev/null 2>&1
ldd (GNU libc) 2.17
hostguard starting ...
not target os, no need config dependent
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
192.168.0.131 remote_install finished. [OK]
==================
```

Step 11 Wait for 5 to 10 minutes and return to the HSS console. On the **Server Install & Config** page, click the **Agents** tab, and click **Servers with Agents**. Check the agent status of the target server.

If the **Agent Status** is **Online**, the agent has been installed.

----End

Installing the Agent on Multiple Third-party Linux Servers Using Commands

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **Third-party Cloud or Data Center Server** and click **Configure Now**.

Step 8 Select an installation method.

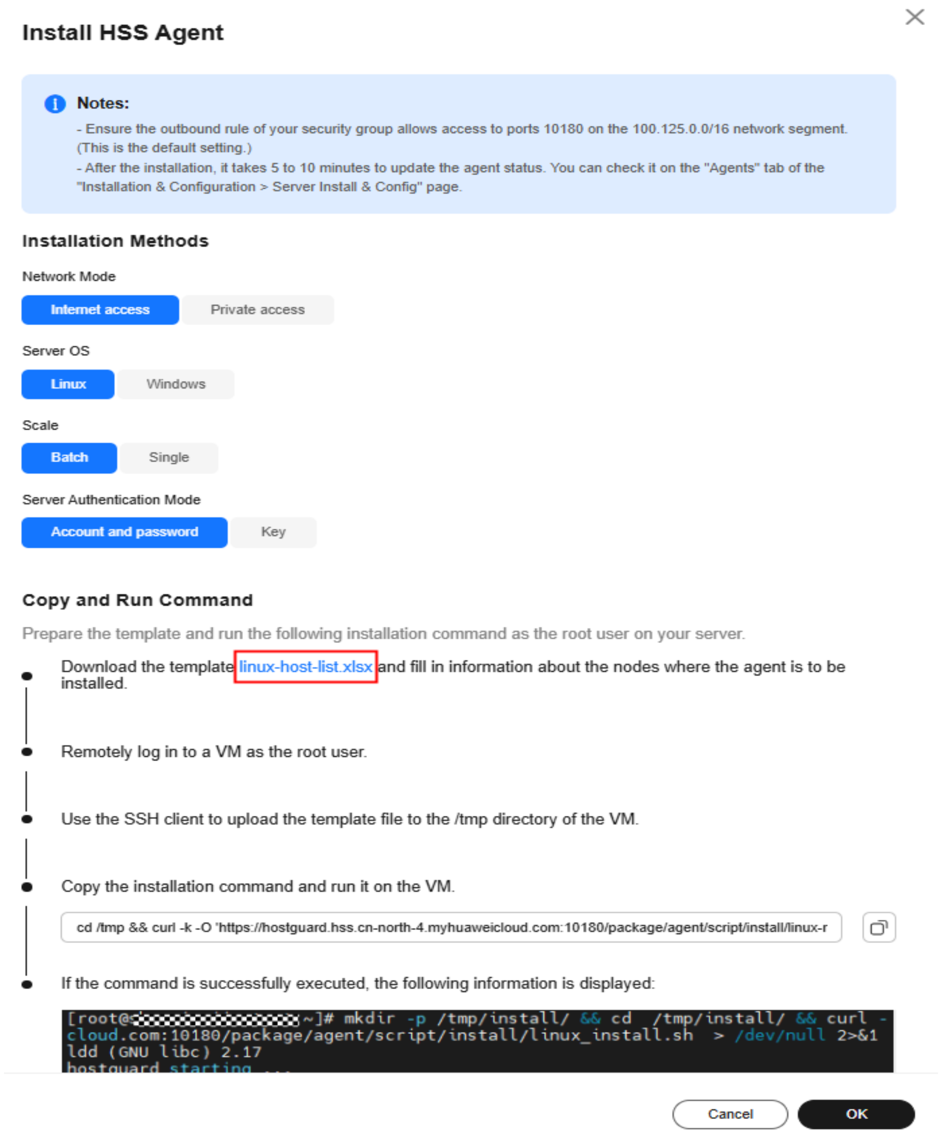
- **Network Mode**: **Internet access**
- **Server OS**: **Linux**
- **Scale**: **Batch**
- **Server Authentication Mode**: Select **Account and password** or **Key** as needed.

Step 9 Install the agent as prompted.

Perform the following operations on any server.

1. On the console, click **linux-host-list.csv** in the **Install HSS Agent** dialog box to download the template.

Figure 2-32 Downloading linux-host-list.csv



Install HSS Agent

Notes:
- Ensure the outbound rule of your security group allows access to ports 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Agents" tab of the "Installation & Configuration > Server Install & Config" page.

Installation Methods

Network Mode: Internet access

Server OS: Linux

Scale: Batch

Server Authentication Mode: Account and password

Copy and Run Command

Prepare the template and run the following installation command as the root user on your server.

- Download the template linux-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Remotely log in to a VM as the root user.
- Use the SSH client to upload the template file to the /tmp directory of the VM.
- Copy the installation command and run it on the VM.

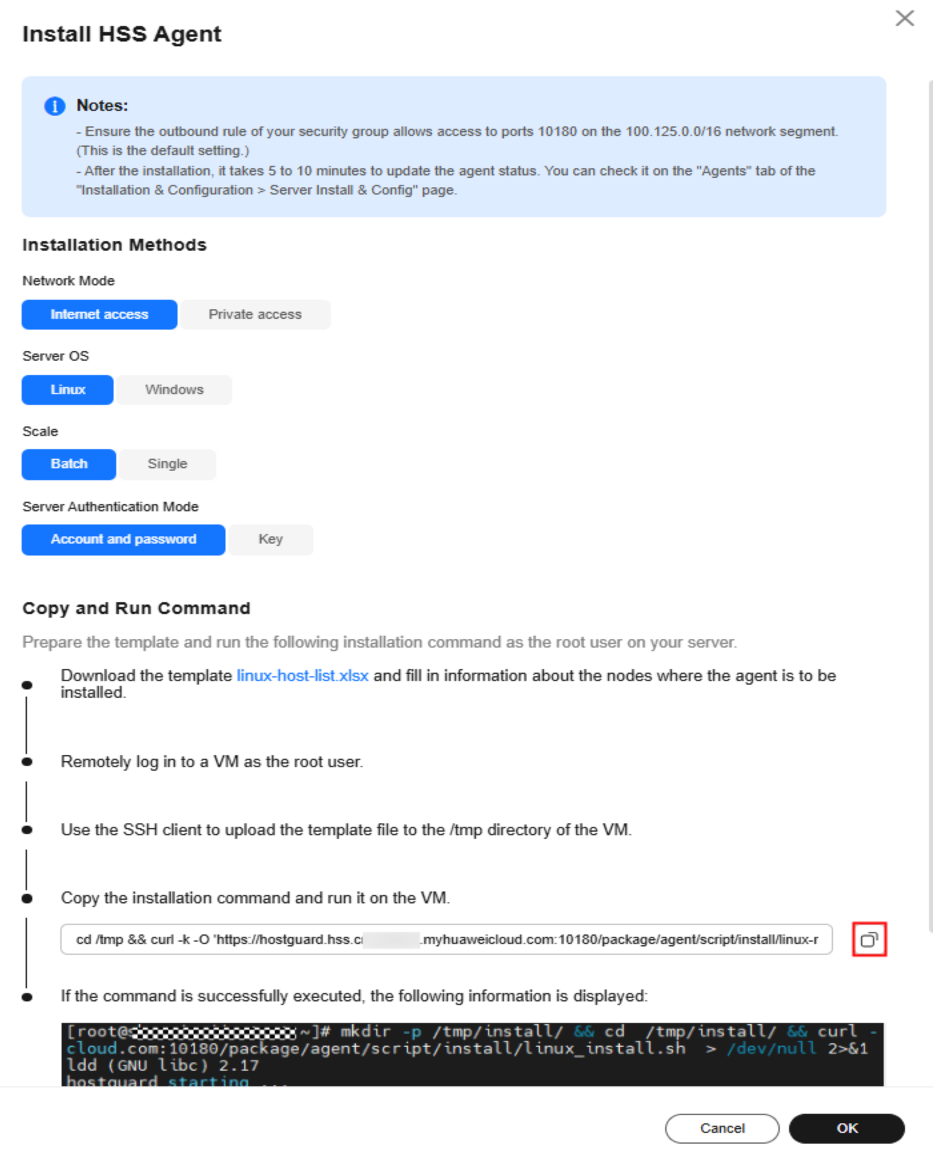
```
cd /tmp && curl -k -O 'https://hostguard.hss.cn-north-4.myhuaweicloud.com:10180/package/agent/script/install/linux-r
```

- If the command is successfully executed, the following information is displayed:

```
[root@[redacted]~]# mkdir -p /tmp/install/ && cd  /tmp/install/ && curl -
cloud.com:10180/package/agent/script/install/linux_install.sh  > /dev/null 2>&1
ldd (GNU libc) 2.17
hostguard starting ...
```

2. Fill in the server information based on the requirements in the **linux-host-list.csv** template and save it.
3. Use the **root** account to remotely log in to any target server.
4. Use the SSH client to upload the template file **linux-host-list.csv** to the **/tmp** directory on the server.
5. Return to the HSS console and click ⧉ to copy the installation command.

Figure 2-33 Copying the installation command



Install HSS Agent

Notes:
- Ensure the outbound rule of your security group allows access to ports 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Agents" tab of the "Installation & Configuration > Server Install & Config" page.

Installation Methods

Network Mode: Internet access (selected) | Private access

Server OS: Linux (selected) | Windows

Scale: Batch (selected) | Single

Server Authentication Mode: Account and password (selected) | Key

Copy and Run Command

Prepare the template and run the following installation command as the root user on your server.

- Download the template linux-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Remotely log in to a VM as the root user.
- Use the SSH client to upload the template file to the /tmp directory of the VM.
- Copy the installation command and run it on the VM.

```
cd /tmp && curl -k -O 'https://hostguard.hss.c[redacted]myhuaweicloud.com:10180/package/agent/script/install/linux-r
```

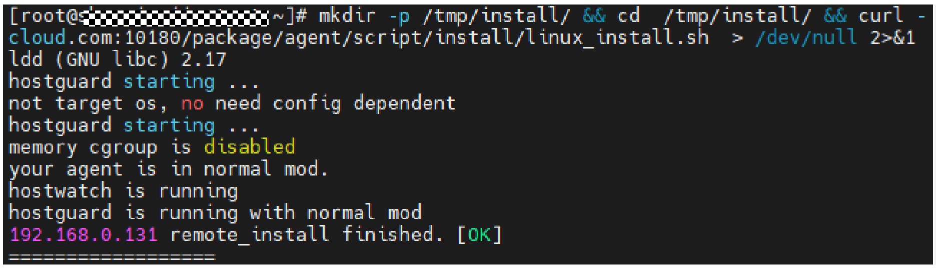
- If the command is successfully executed, the following information is displayed:

```
[root@[redacted]~]# mkdir -p /tmp/install/ && cd  /tmp/install/ && curl -
cloud.com:10180/package/agent/script/install/linux_install.sh  > /dev/null 2>&1
ldd (GNU libc) 2.17
hostguard starting ...
```

6. Paste and run the installation command on the server to install the agent.

   If the command output shown in **Figure 2-34** is displayed, the agent has been installed.

Figure 2-34 Agent installed



```
[root@[redacted]~]# mkdir -p /tmp/install/ && cd  /tmp/install/ && curl -
cloud.com:10180/package/agent/script/install/linux_install.sh  > /dev/null 2>&1
ldd (GNU libc) 2.17
hostguard starting ...
not target os, no need config dependent
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
192.168.0.131 remote_install finished. [OK]
==================
```

7. Wait for 5 to 10 minutes and return to the HSS console. On the **Server Install & Config** page, click the **Agents** tab, and click **Servers with Agents**. Check the agent status of the target server.

If the **Agent Status** is **Online**, the agent has been installed.

----End

Installing the Agent on Third-party Windows Servers Using a Script

The following describes how to install the agent on a Windows server. You can select a method as required.

Installing the Agent on a Single Third-party Windows Server Using a Script

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **Third-party Cloud or Data Center Server** and click **Configure Now**.

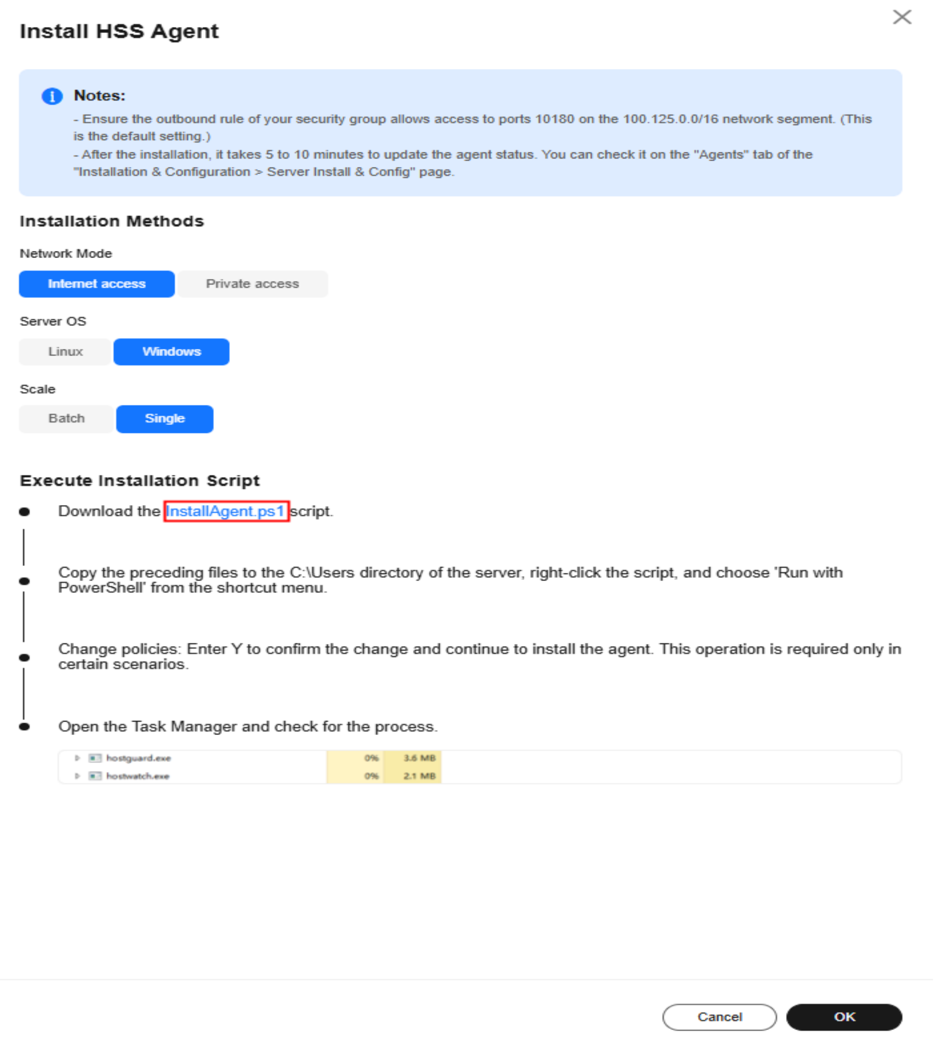
Step 8 Select an installation method.

- **Network Mode**: **Internet access**
- **Server OS**: **Windows**
- **Scale**: **Single**

Step 9 Install the agent as prompted.

1. On the console, click **installAgent.ps1** in the **Install HSS Agent** dialog box to download the installation script.

Figure 2-35 Downloading installAgent.ps1



Install HSS Agent

Notes:

- Ensure the outbound rule of your security group allows access to ports 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Agents" tab of the "Installation & Configuration > Server Install & Config" page.

Installation Methods

Network Mode: Internet access (selected) | Private access

Server OS: Linux | Windows (selected)

Scale: Batch | Single (selected)

Execute Installation Script

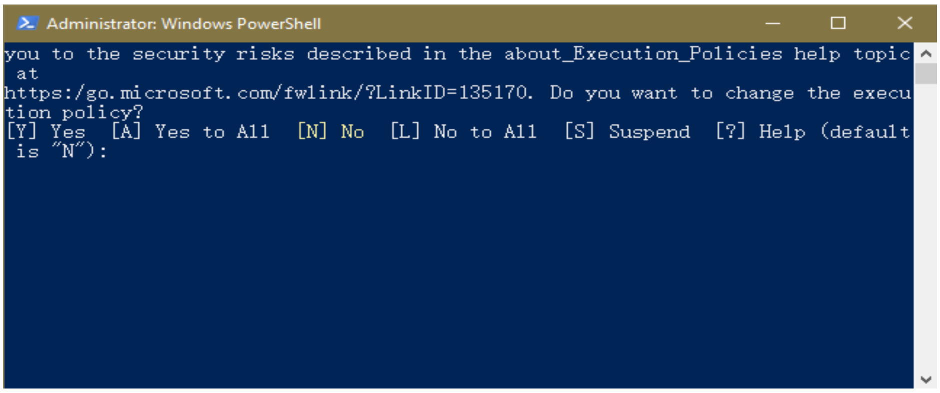
- Download the InstallAgent.ps1 script.
- Copy the preceding files to the C:\Users directory of the server, right-click the script, and choose 'Run with PowerShell' from the shortcut menu.
- Change policies: Enter Y to confirm the change and continue to install the agent. This operation is required only in certain scenarios.
- Open the Task Manager and check for the process.

```
hostguard.exe    0%   3.6 MB
hostwatch.exe    0%   2.1 MB
```

2. Copy the **installAgent.ps1** file to the **C:\Users** directory of the server where the agent is to be installed.
3. Right-click **installAgent.ps1** and choose **Run with PowerShell**.
4. (Optional) In the dialog box that is displayed, enter **Y** to run the script to install the agent.

   If no dialog box is displayed, skip this step.

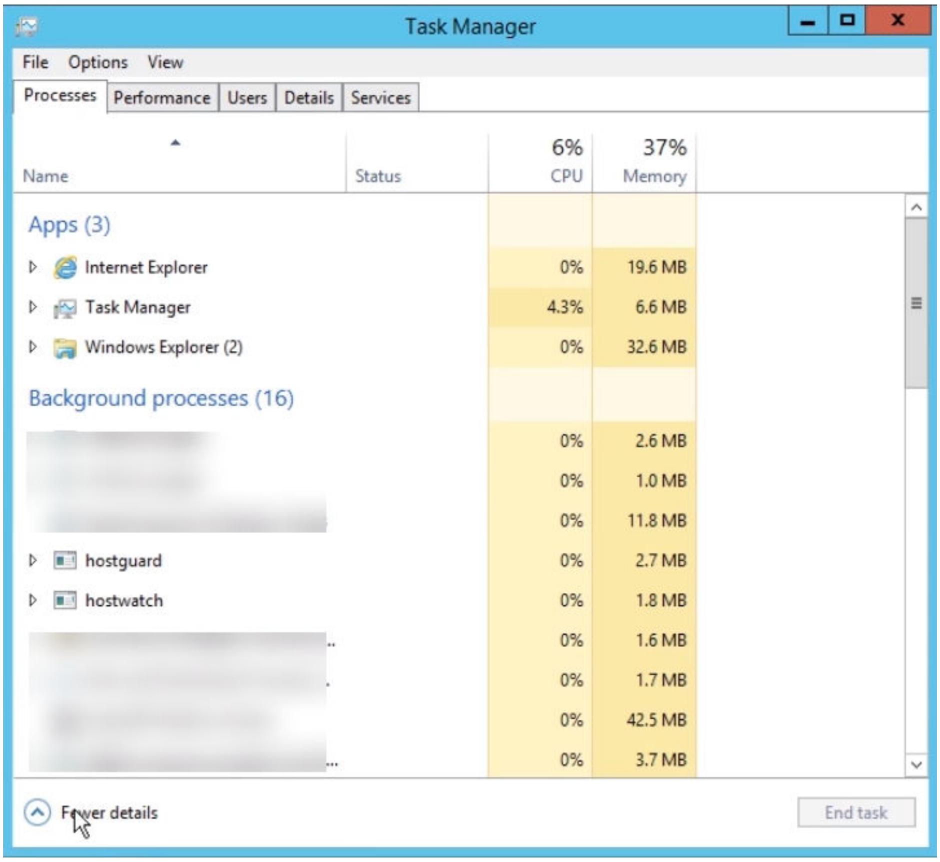
Figure 2-36 Changing the execution policy



```
you to the security risks described in the about_Execution_Policies help topic
 at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execu
tion policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default
 is "N"):
```

5. After the execution, open the Task Manager and check whether **hostguard.exe** and **hostwatch.exe** exist. If they do, the agent has been installed.

Figure 2-37 Agent installed



Name	Status	6% CPU	37% Memory
Apps (3)			
Internet Explorer		0%	19.6 MB
Task Manager		4.3%	6.6 MB
Windows Explorer (2)		0%	32.6 MB
Background processes (16)			
[redacted]		0%	2.6 MB
[redacted]		0%	1.0 MB
[redacted]		0%	11.8 MB
hostguard		0%	2.7 MB
hostwatch		0%	1.8 MB
[redacted]		0%	1.6 MB
[redacted]		0%	1.7 MB
[redacted]		0%	42.5 MB
[redacted]		0%	3.7 MB

6. Wait for 5 to 10 minutes and return to the HSS console. On the **Server Install & Config** page, click the **Agents** tab, and click **Servers with Agents**. Check the agent status of the target server.

   If the **Agent Status** is **Online**, the agent has been installed.

----End

Installing the Agent on Multiple Third-party Windows Servers Using a Script

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Agents** tab.

Step 6 In the upper right corner of the page, click **Install HSS Agent**.

Step 7 Select **Third-party Cloud or Data Center Server** and click **Configure Now**.

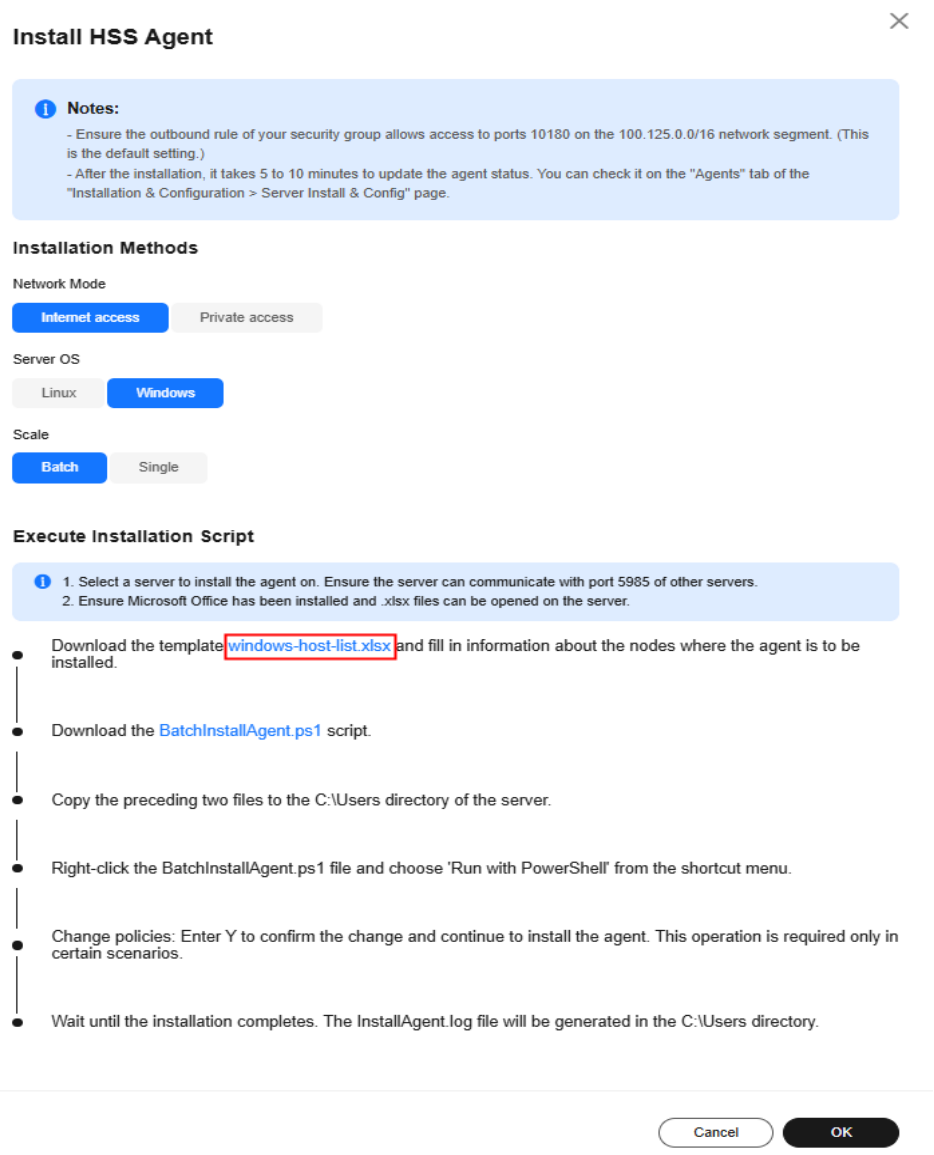
Step 8 Select an installation method.

- **Network Mode**: **Internet access**
- **Server OS**: **Windows**
- **Scale**: **Batch**

Step 9 Install the agent as prompted.

1. On the console, click **windows-host-list.xlsx** in the **Install HSS Agent** dialog box to download the template to the local PC.

Figure 2-38 Downloading windows-host-list.xlsx



Install HSS Agent

Notes:
- Ensure the outbound rule of your security group allows access to ports 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Agents" tab of the "Installation & Configuration > Server Install & Config" page.

Installation Methods

Network Mode: Internet access (selected) | Private access

Server OS: Linux | Windows (selected)

Scale: Batch (selected) | Single

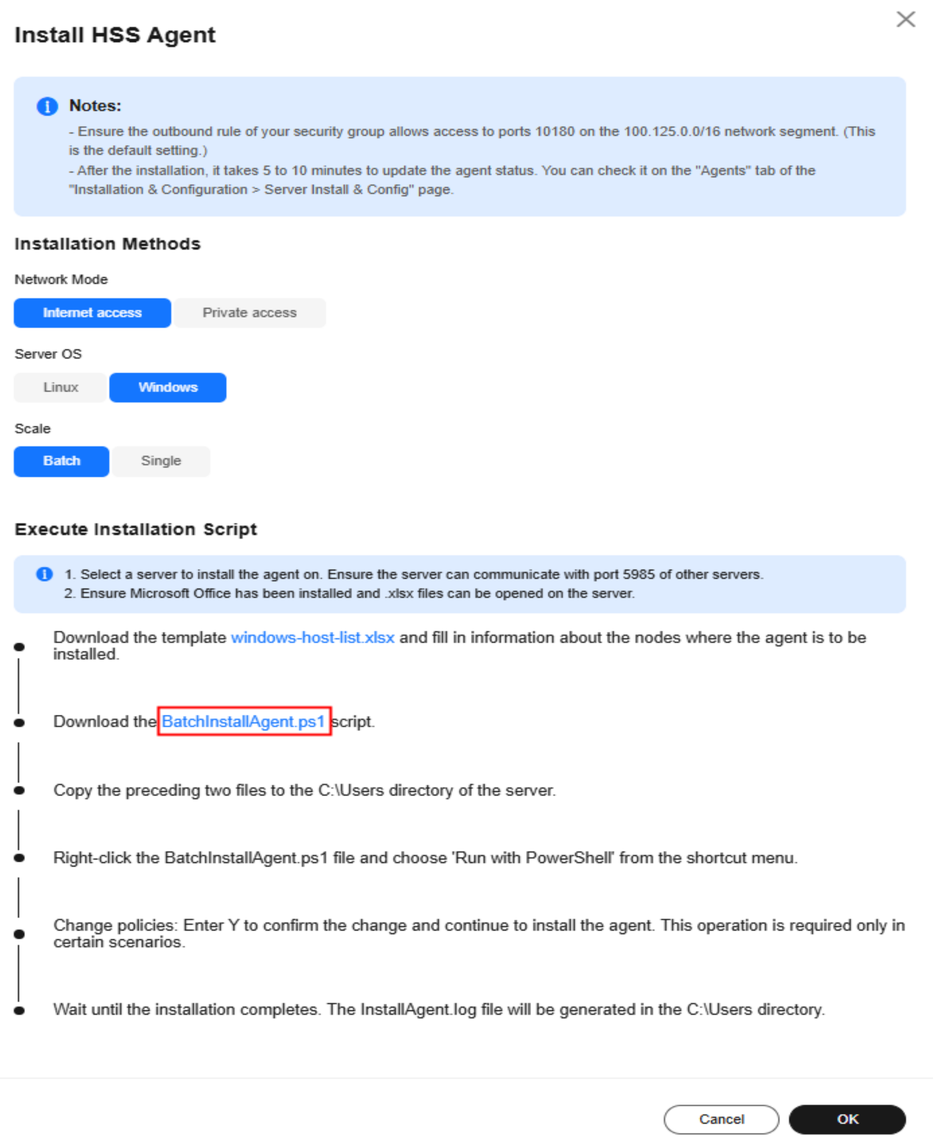
Execute Installation Script

1. Select a server to install the agent on. Ensure the server can communicate with port 5985 of other servers.
2. Ensure Microsoft Office has been installed and .xlsx files can be opened on the server.

- Download the template windows-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Download the BatchInstallAgent.ps1 script.
- Copy the preceding two files to the C:\Users directory of the server.
- Right-click the BatchInstallAgent.ps1 file and choose 'Run with PowerShell' from the shortcut menu.
- Change policies: Enter Y to confirm the change and continue to install the agent. This operation is required only in certain scenarios.
- Wait until the installation completes. The InstallAgent.log file will be generated in the C:\Users directory.

2. Enter server information based on the requirements in the **windows-host-list.xlsx** template and save it.
3. Return to the HSS console and click **BatchInstallAgent.ps1** to download the installation script.

Figure 2-39 Downloading BatchInstallAgent.ps1



Install HSS Agent

Notes:
- Ensure the outbound rule of your security group allows access to ports 10180 on the 100.125.0.0/16 network segment. (This is the default setting.)
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Agents" tab of the "Installation & Configuration > Server Install & Config" page.

Installation Methods

Network Mode: Internet access (selected) | Private access

Server OS: Linux | Windows (selected)

Scale: Batch (selected) | Single

Execute Installation Script

1. Select a server to install the agent on. Ensure the server can communicate with port 5985 of other servers.
2. Ensure Microsoft Office has been installed and .xlsx files can be opened on the server.

- Download the template windows-host-list.xlsx and fill in information about the nodes where the agent is to be installed.
- Download the BatchInstallAgent.ps1 script.
- Copy the preceding two files to the C:\Users directory of the server.
- Right-click the BatchInstallAgent.ps1 file and choose 'Run with PowerShell' from the shortcut menu.
- Change policies: Enter Y to confirm the change and continue to install the agent. This operation is required only in certain scenarios.
- Wait until the installation completes. The InstallAgent.log file will be generated in the C:\Users directory.

4. Copy the **windows-host-list.xlsx** and **BatchInstallAgent.ps1** files to the **C:\Users\Administrator** directory on any of the servers where the agent is to be installed.

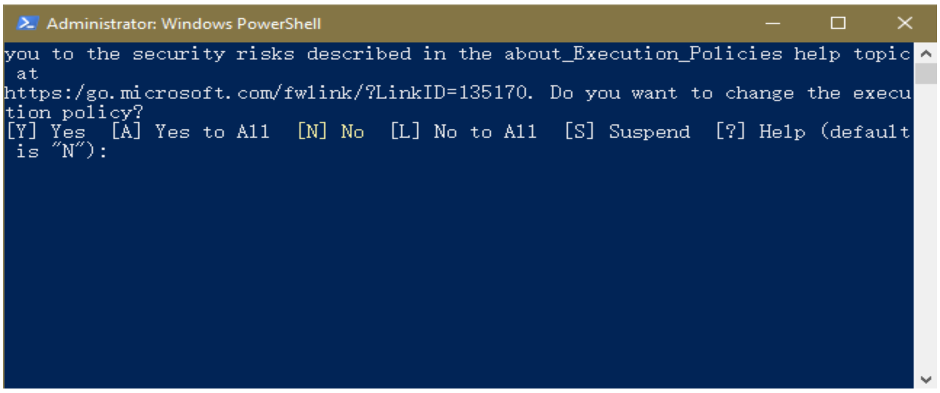
   Ensure that the port 5985 of the server is connected to that port of other servers where the agent is to be installed.

5. Right-click **BatchInstallAgent.ps1** and choose **Run with PowerShell**.

6. (Optional) In the dialog box that is displayed, enter **Y** to run the script to install the agent.

   If no dialog box is displayed, skip this step.

Figure 2-40 Changing the execution policy



```
you to the security risks described in the about_Execution_Policies help topic
 at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execu
tion policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default
 is "N"):
```

7. After the script is executed successfully, check whether the **BatchInstallAgent.log** file exists in **C:\Users\Administrator**.

   If the **BatchInstallAgent.log** file exists, the agent has been installed.

8. Wait for 5 to 10 minutes and return to the HSS console. On the **Server Install & Config** page, click the **Agents** tab, and click **Servers with Agents**. Check the agent status of the target server.

   If the **Agent Status** is **Online**, the agent has been installed.

----End

FAQ

For details about how to troubleshoot the agent installation failure, see **What Should I Do If Agent Installation Failed?**

Follow-up Procedure

After the agent is installed on the server or container node, **enable protection**.

2.4 Enabling Protection

To enable protection, allocate a quota to a server or a container. After protection is disabled or the protected server or container is removed, the quota can be allocated to another server or container.

Prerequisites

- HSS can be billed in yearly/monthly or pay-per-use mode. To use yearly/monthly billing, ensure you have purchased sufficient protection quotas. For details, see **Purchasing an HSS Quota**. If you use the pay-per-use billing mode, you do not need to purchase quotas in advance.
- Ensure that the agent has been installed on the server or container node and is online. For details, see **Installing the Agent on Huawei Cloud Servers** and **Installing the Agent on Third-party Servers**.

Constraints

- Server

Before you enable protection for a Windows server, enable the Windows firewall to block the source IP addresses of brute-force attacks. If the Windows firewall is not enabled, HSS only generates alarms for detected brute-force attacks, but does not block them.

  - After the Windows firewall is enabled, every time HSS detects a brute-force attack, it adds an inbound rule to the firewall to block the attack source IP address. There are no other impacts on services.
  - Do not disable the Windows firewall when using HSS, or HSS cannot block the source IP addresses of brute-force attacks. Once it is disabled, HSS may fail to block the attack source IP addresses even after you manually enable it again.

- Container

  HSS can only protect Docker, Containerd, CRI-O, Podman, and iSulad containers.

Enabling Protection

Perform the following operations to enable protection based on the edition you need.

Enabling the Basic/Professional/Enterprise/Premium Edition

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

NOTE

The server list displays the protection status of only the following servers:

- Huawei Cloud servers purchased in the selected region
- Non-Huawei Cloud servers that have been added to the selected region

Step 4 Locate a server whose agent status is **Online**.

Step 5 Click **Enable** in the **Operation** column of a server.

Step 6 Confirm the server information and select a billing mode.

You can buy HSS in the pay-per-use or yearly/monthly mode.

- **Yearly/Monthly**
  - **Billing Mode**: Select **Yearly/Monthly**.
  - **Edition**: Select an edition.
  - **Select Quota**: Select a quota allocation mode.
    - **Select a quota randomly**: Let the system allocate the quota with the longest remaining validity to the server.
    - Select a quota ID and allocate it to a server.

- **Pay-per-use**
  - **Billing Mode**: Select **Pay-per-use**.
  - **Edition**: Select an edition.
  - **Tags**: Select a tag if you want to use it to identify multiple types of cloud resources.

⚠ CAUTION

If the version of the agent installed on the Linux server is 3.2.10 or later or the version of the agent installed on the Windows server is 4.0.22 or later, ransomware prevention is automatically enabled with the premium edition. Deploy honeypot files on servers and automatically isolate suspicious encryption processes (there is a low probability that processes are incorrectly isolated). You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Enabling Ransomware Backup**.

Step 7 Read the *Host Security Service Disclaimer* and select **I have read and agree to the Host Security Service Disclaimer**.

Step 8 Click **OK**. If the **Protection Status** of the target server is **Enabled**, the basic, professional, enterprise or premium edition has been enabled.

NOTE

- Alternatively, on the **Quotas** tab of the **Servers & Quota** page, click **Bind Server** in the **Operation** column to bind a quota to a server. HSS will automatically enable protection for the server.
- A quota can be bound to a server to protect it, on condition that the agent on the server is online.
- After HSS is enabled, it will scan your servers for security issues. Check items vary according to the edition you enabled.

  For details about the differences between the editions, see **Features**.

----End

Enabling Web Tamper Protection

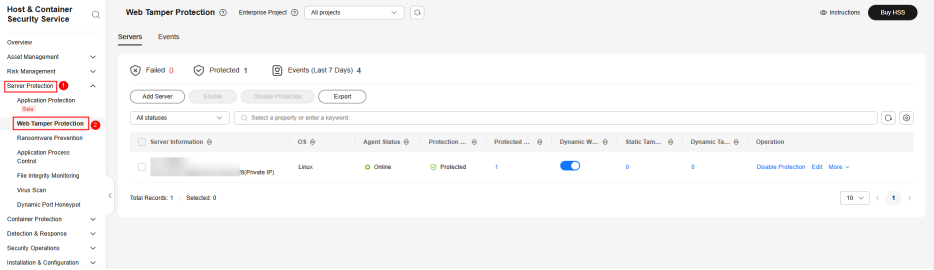
WTP can be enabled for one or multiple servers at a time. When you enable WTP for multiple servers at a time, the same protected directory settings will be applied to all of them, and cannot be customized for each server. If these servers have different directories to be protected, you can customize the protected directories or other settings for them separately after WTP is enabled. For details, see **Modifying WTP Configuration**.

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

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Figure 2-41 Web tamper protection



Failed 0 Protected 1 Events (Last 7 Days) 4

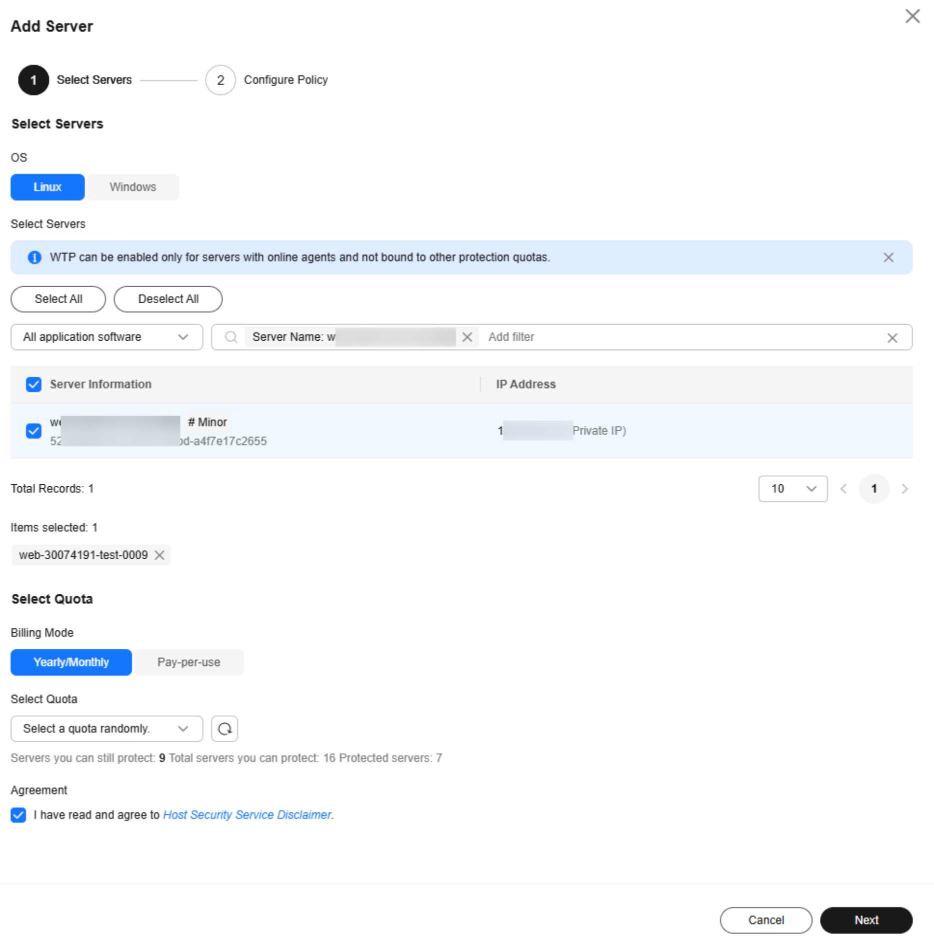
Server Information	OS	Agent Status	Protection ...	Protected ...	Dynamic W...	Static Tam...	Dynamic Ta...	Operation
8(Private IP)	Linux	Online	Protected	1	●	0	0	Disable Protection Edit More

Total Records: 1 Selected: 0

Step 4 On the **Servers** tab, click **Add Server**. The **Add Server** page is displayed.

Step 5 On the **Add Server** page, select servers and click **Next**. For more information, see **Table 2-8**.

Figure 2-42 Selecting servers



WTP can be enabled only for servers with online agents and not bound to other protection quotas.

Server Name: w

☑ Server Information	IP Address
☑ w # Minor 52 d-a4f7e17c2655	1 Private IP)

Total Records: 1

Items selected: 1

web-30074191-test-0009

Select a quota randomly.

Servers you can still protect: 9 Total servers you can protect: 16 Protected servers: 7

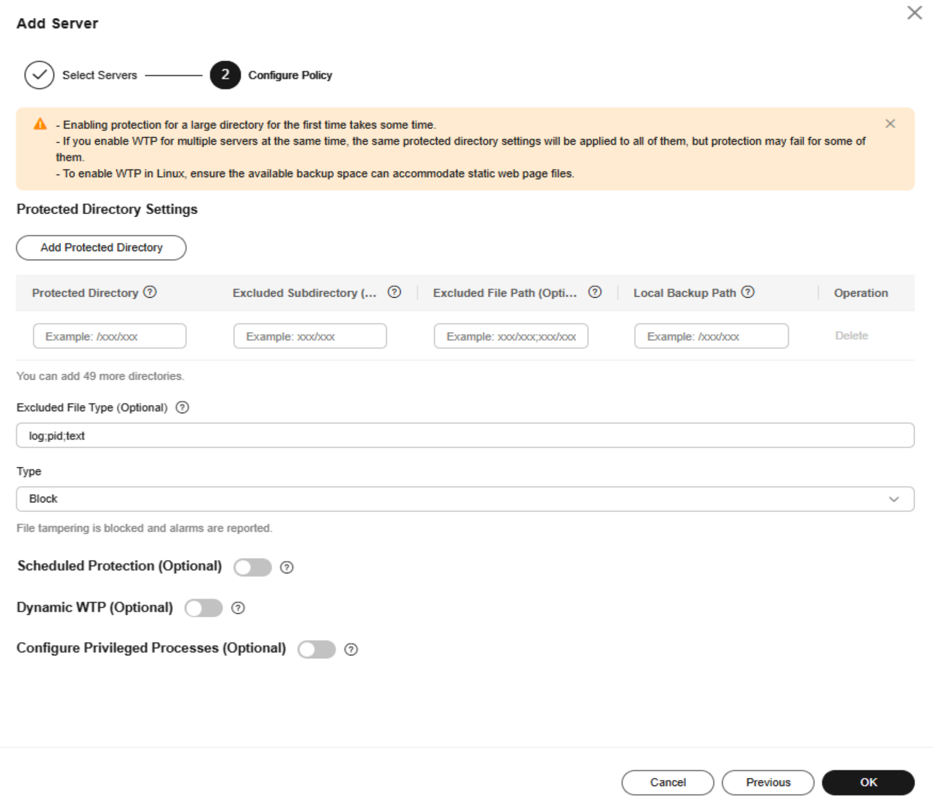
☑ I have read and agree to *Host Security Service Disclaimer*.

Table 2-8 Parameters for selecting protected servers

Parameter	Description	Example Value
OS	Select the OS type of the server to be protected by WTP. ● Linux ● Windows	Linux
Select Servers	Select servers. You can filter the servers by software type or other attributes.	-
Select Quota	The HSS WTP edition supports two billing modes, yearly/monthly and pay-per-use billing, to meet requirements in different scenarios. ● Yearly/Monthly billing is a prepaid mode in which you pay for the service before using it. Your bill is generated based on the required duration you specify in the order. The longer you use the service, the more discounts you got. ● Pay-per-use is a postpaid billing mode. You pay as you go and just pay for what you use. The HSS usage is calculated by the second but billed every hour. With the pay-per-use billing mode, you can easily adapt to resource requirement changes, reducing the risk of over-provisioning resources or lacking capacity. In this mode, there are no upfront commitments required. When selecting the yearly/monthly billing mode, you can select a quota or retain the default value **Select a quota randomly**.	Yearly/Monthly
Agreement	Before enabling WTP, ensure that you have read the *Host Security Service Disclaimer*. Select **I have read and agree to the *Host Security Service Disclaimer***.	Selected

Step 6 On the **Add Server** page, configure policies. For more information, see **Table 2-9**.

Figure 2-43 Configuring policies



Add Server

Select Servers — 2 Configure Policy

- Enabling protection for a large directory for the first time takes some time.
- If you enable WTP for multiple servers at the same time, the same protected directory settings will be applied to all of them, but protection may fail for some of them.
- To enable WTP in Linux, ensure the available backup space can accommodate static web page files.

Protected Directory Settings

Add Protected Directory

Protected Directory	Excluded Subdirectory (...	Excluded File Path (Opti...	Local Backup Path	Operation
Example: /xxx/xxx	Example: xxx/xxx	Example: xxx/xxx;xxx/xxx	Example: /xxx/xxx	Delete

You can add 49 more directories.

Excluded File Type (Optional): log;pid;text

Type: Block

File tampering is blocked and alarms are reported.

Scheduled Protection (Optional)

Dynamic WTP (Optional)

Configure Privileged Processes (Optional)

Table 2-9 Parameters for configuring rules

Parameter	Description	Example Value
Protected Directory	WTP supports static and dynamic web page protection. Static WTP protects specified directories by locking files in the web file directory in the drive to prevent attackers from modifying the files. Therefore, when configuring a protection policy, you need to specify the directories to be protected. After a directory is protected, the files and folders in the directory will become read-only. The requirements for adding a protected directory are as follows: ● For Linux, – It cannot start with a space, end with a slash (/), or contain semi-colons (;). Up to 256 characters are allowed. – A server can have up to 50 protected directories. – The folder levels of a protected directory cannot exceed 100. – The total folders in protected directories cannot exceed 900,000. ● For Windows, – Up to 256 characters are allowed. The directory name cannot start with a space or end with a backslash (\). It cannot contain the following characters: ;/*?"<>| – A server can have up to 50 protected directories. **Do not add network directories as protected directories.** The reasons are as follows: 1. A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. 2. The access to network directories may occupy all your bandwidth and affect your services.	● Linux: **/etc/lesuo** ● Windows: **d:\web**

Parameter	Description	Example Value
Excluded Subdirectory (Optional)	If a protected directory contains subdirectories that do not need to be protected, you can exclude the subdirectories. The requirements for adding a subdirectory are as follows: ● A subdirectory name must be a valid relative path of the protected directory. ● A subdirectory name cannot start or end with a slash (/), and can contain up to 256 characters. ● Up to 10 subdirectories can be added. Use semicolons (;) to separate multiple subdirectories.	● Linux: **lesuo/test** ● Windows: **web\test**
Excluded File Path (Optional)	This item is available only for Linux servers. If a protected directory contains files that do not need to be protected, exclude the files. The requirements for adding excluded file paths are as follows: ● A file path must be a valid relative path of the protected directory. ● A file path cannot start or end with a slash (/), and can contain up to 256 characters. ● Up to 50 file paths can be added. Use semicolons (;) to separate multiple file paths.	lesuo/data;lesuo/ma.txt

Parameter	Description	Example Value
Local Backup Path	This item is available only for Linux servers. Set a local backup path for a protected directory. After WTP is enabled, files in the protected directory are automatically backed up to the local backup path. Once the system detects that a file in the protected directory is tampered with, it immediately uses the local backup to restore the tampered file. The requirements for adding local backup paths are as follows: ● A local backup path cannot contain semicolons (;), start with a space, or end with a slash (/). Up to 256 characters are allowed. ● Key system directories are a main attack target and cannot be used as backup paths, including but not limited to **/etc/**, **/bin/**, **/usr/bin/**, **/var/spool/**, **/usr/sbin/**, **/sbin/**, **/usr/lib/**, **/lib/**, **/lib64/**, **/usr/lib64/**, and their subdirectories. Local backup rule description: ● 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.	/etc/backup
Excluded File Type	If a protected directory contains files of certain types that do not need to be protected, exclude these file types, for example, logs. You can exclude any type of files. To record the running status of servers in real time, exclude the log files in the protected directory. You can set high permission requirements for log read and write, so that attackers cannot view or tamper with log files.	log

Parameter	Description	Example Value
Type	Action taken when file tampering is detected. - **Alarm**: Only alarms are reported. - **Block**: An alarm is reported, and the file is restored to the status before being tampered with.	Block
Scheduled Protection (Optional)	You can schedule when to disable static WTP. In the unprotected period, you can modify, update, or release web pages. Click to enable scheduled protection and configure the following parameters: - **Unprotected Time Range** A time range when WTP is disabled within a day, for example, 10:05 to 15:35. Requirements: – A time range must be at least 5 minutes. – Time ranges (except for those starting at 00:00 or ending at 23:59) cannot overlap and must have at least a 5-minute interval. – All time ranges are subject to the system time of the server. - **Unprotected Days of a Week** Static WTP is automatically disabled on specified days of a week, for example, Wednesday and Thursday.	, 10:05-15:35, Wednesday
Dynamic WTP (Optional)	Dynamic WTP is mainly used to protect Tomcat applications on Linux. It can detect and prevent tampering with dynamic data, such as database data, in real time during application running. Currently, dynamic WTP can protect Tomcat applications using JDK 8, JDK 11, and JDK 17. To enable dynamic WTP, click and enter a complete Tomcat bin directory path, for example, **/usr/workspace/apache-tomcat-8.5.15/bin**. The system presets the **setenv.sh** script in the bin directory to configure the startup parameters of the anti-tamper program.	, /usr/workspace/apache-tomcat-8.5.15/bin

Parameter	Description	Example Value
Configure Privileged Processes (Optional)	A privileged process is a process authorized to modify a protected directory. After WTP is enabled, all files in the protected directory will be set to read-only and cannot be modified. If anyone attempts to modify a file or website, the system will automatically restore it to the status before the modification. You can add privileged processes and use them to modify the files in protected directories or update websites. Ensure the specified privileged processes, which are authorized to access protected directories, are secure and reliable. This feature is compatible with Linux and Windows. For Linux, only the distributions using kernel versions 5.10 or later are supported. Click ○ to enable the privileged processes and configure the following parameters: ● **Process File Path** Set one or multiple complete file paths of privileged processes. Put each privileged process file path on a separate line. Up to 10 privileged processes are allowed. ● **Trust Subprocess** If **Trust Subprocess** is enabled, HSS will trust all the subprocesses up to five levels deep in the subdirectories of specified directories, and allow the subprocesses to modify protected directories, and allow the subprocesses to modify protected directories.	● Linux: **/Path/Software.type** ● Windows: **C:\Path\Software.type**

Step 7 After the policy is configured, click **OK**.

Step 8 On the **Servers** tab, check the static and dynamic WTP status of the server.

The **Protected** status indicates protection has been enabled. After dynamic WTP is enabled, restart Tomcat to apply the settings.

----End

Enabling Container Protection

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

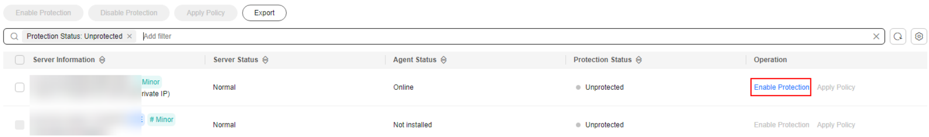
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**.

Step 4 In the row of a server, click **Enable Protection** in the **Operation** column. The confirmation dialog box is displayed.

By default, only the Linux servers where the agent is installed (that is, the servers eligible for the container edition) are displayed in the list. To install the agent on a server, perform the operations in **Installing the Agent on Servers** and **Installing an Agent in a Cluster**.

Figure 2-44 Enabling container protection



□ Server Information	Server Status	Agent Status	Protection Status	Operation
□ [redacted] Minor rivate IP)	Normal	Online	● Unprotected	Enable Protection Apply Policy
□ [redacted] # Minor	Normal	Not installed	● Unprotected	Enable Protection Apply Policy

Step 5 Confirm the node information and select a billing mode.

You can buy quota in pay-per-use or yearly/monthly mode.

- **Yearly/Monthly**
  - **Billing Mode**: Select **Yearly/Monthly**.
  - **Select Quota**: Select a quota allocation mode.
    - **Random quota**: Let the system allocate the quota with the longest remaining validity to the server.
    - Select a quota ID and allocate it to a server.
- **Pay-per-use**
  - **Billing Mode**: Select **Pay-per-use**.
  - **Tags**: Select a tag if you want to use it to identify multiple types of cloud resources.

⚠ CAUTION

- A container security quota protects one cluster node.
- If the version of the agent installed on the Linux server is 3.2.10 or later or the version of the agent installed on the Windows server is 4.0.22 or later, ransomware prevention is automatically enabled with the container edition. Deploy honeypot files on servers and automatically isolate suspicious encryption processes (there is a low probability that processes are incorrectly isolated). You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Enabling Ransomware Backup**.

Step 6 Read the *Host Security Service Disclaimer* and select **I have read and agree to the Container Guard Service Disclaimer**.

Step 7 Click **OK**. If the **Protection Status** of the node changes to **Protected**, protection has been enabled.

----End

Viewing Scan Details

After server protection is enabled, HSS will immediately perform a comprehensive scan on the server. It may take a long time. After the scan is complete, you can check its details.

Step 1 Choose **Asset Management** > **Servers & Quota**. Locate the server on the **Servers** tab page.

Step 2 Check the **Risk Level** column of the server.

Table 2-10 Risk status

Status	Description
Pending risk detection	The server is neither protected nor scanned.
Safe	No risks were found in the comprehensive scan on the server; or the protection has just been enabled, and no risks have been found yet.
Risky	The server has security risks.

Step 3 Hover the cursor over the risk status to view the risk distribution.

You can click a value to go to the details page.

----End

Follow-up Procedure

HSS provides server and container defense functions for you to enable as needed. For more information, see **Manual configurations**.

Table 2-11 Manual configurations

Category	Function	Reference
Security Configurations	● Common login location/IP address ● SSH login IP address whitelist ● Isolate and kill malicious programs	**Common Security Configuration**

Category	Function	Reference
Server Protection	• Application protection • Ransomware prevention • Application process control • File integrity monitoring (FIM) • Virus scan • Dynamic port honeypot	**Server Protection**
Container Protection	• Container firewall • Container cluster protection	**Container Protection**
Policy Management	Policy management includes asset management, baseline inspection, intrusion detection, and self-protection policies. Intrusion detection is disabled by default. You can enable and modify them as needed.	**Policy Management**

2.5 Enabling Alarm Notifications

After alarm notification is enabled, you can receive alarm notifications sent by HSS to learn about security risks facing your servers and web pages. Without this function, you have to log in to the management console to view alarms.

- Alarm notification settings are effective only for the current region. To receive notifications from another region, switch to that region and configure alarm notification.
- Alarm notifications may be mistakenly blocked. If you have enabled notifications but not received any, check whether they have been blocked as spam.

- The Simple Message Notification (SMN) service is a paid service. For details about the price, see **Product Pricing Details**.

Enabling Alarm Notifications

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

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

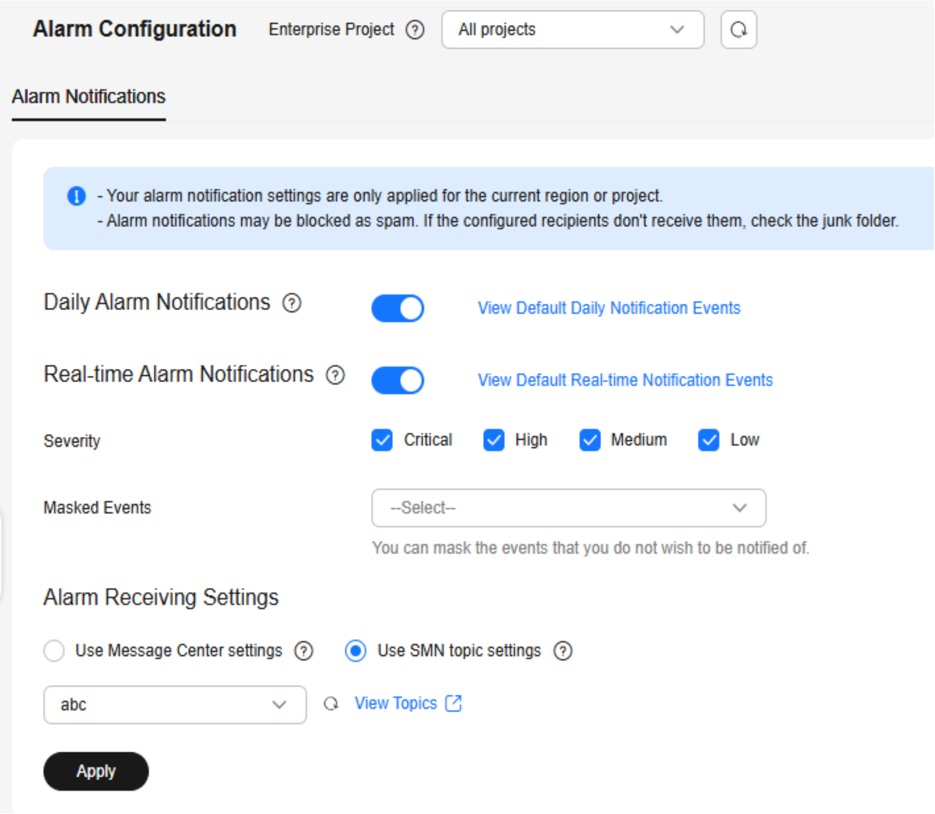
Step 3 In the navigation pane, choose **Installation & Configuration** > **Alarm Notifications**.

Step 4 (Optional) If your servers are managed by enterprise projects, you can select an enterprise project to configure alarm notifications.

- If you select a single enterprise project, the alarm notification information takes effect only in the corresponding enterprise project.
- If you select **All projects**, the alarm notification information takes effect in all enterprise projects.

Step 5 Configure the alarm notification parameters as prompted. For more information, see **Table 2-12**.

Figure 2-45 Alarm configurations



Alarm Configuration Enterprise Project: All projects

Alarm Notifications

- Your alarm notification settings are only applied for the current region or project.
- Alarm notifications may be blocked as spam. If the configured recipients don't receive them, check the junk folder.

Daily Alarm Notifications: on — View Default Daily Notification Events

Real-time Alarm Notifications: on — View Default Real-time Notification Events

Severity: ☑ Critical ☑ High ☑ Medium ☑ Low

Masked Events: --Select--

You can mask the events that you do not wish to be notified of.

Alarm Receiving Settings

○ Use Message Center settings ● Use SMN topic settings

abc — View Topics

Apply

Table 2-12 Alarm configurations

Type	Description	Suggestion
Daily alarm notification	HSS scans the accounts, web directories, vulnerabilities, malicious programs, and key configurations in the server system at 00:00 every day, and sends the summarized detection results to the recipients you set in the Message Center or SMN, depending on which one you chose. To view notification items, click **View Default Daily Notification Events**.	● It is recommended that you receive and periodically check all the content in the daily alarm notification to eliminate risks in a timely manner. ● Daily alarm notifications contain a lot of check items. If you want to send the notifications to recipients set in an SMN topic, you are advised to set the topic protocol to **Email**.
Real-time alarm notification	When an attacker intrudes a server, alarms are sent to the recipients you set in the Message Center or SMN, depending on which one you chose. To view notification items, click **View Default Real-time Notification Events**.	● It is recommended that you receive all the content in the real-time alarm notification and view them in time. The HSS system monitors the security of servers in real time, detects the attacker's intrusion, and sends real-time alarm notifications for you to quickly handle the problem. ● Real-time alarm notifications are about urgent issues. If you want to send the notifications to recipients set in an SMN topic, you are advised to set the topic protocol to **SMS**.
Severity	Select the severities of alarms that you want to be notified of.	All
Masked Events	Select the events that you do not wish to be notified of. Select events to be masked from the drop-down list box.	Determine the events to be masked based on the description in **Alarm Notifications**.

Step 6 Select the alarm notification mode.

- **Use Message Center settings**

  By default, alarm notifications are sent to the contacts under the account. Notification modes include email, SMS, system notification, and group chatbots (WeCom, DingTalk, Feishu, and WeLink). For more information, see **Message Center**.

To configure the notification mode and recipients, perform the following steps:

a. Log in to the management console.

b. Click in the upper right corner to access the Message Center.

   You can view all system notifications on this page.

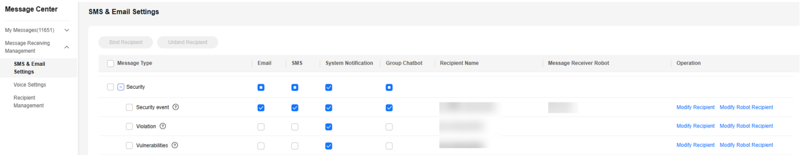
c. In the navigation pane on the left, choose **Message Receiving Management** > **SMS & Email Settings**.

d. Choose **Message Type** > **Security** > **Security event**.

e. Select notification modes as required.

   You can select **Email**, **SMS**, **System Notification**, and **Group Chatbot** (WeCom, DingTalk, Feishu, and WeLink).

Figure 2-46 Configuring notification modes



Message Type	Email	SMS	System Notification	Group Chatbot	Recipient Name	Message Receiver Robot	Operation
Security	■	■	☑	■			
Security event	☑	☑	☑	☑	[redacted]	[redacted]	Modify Recipient Modify Robot Recipient
Violation	□	□	☑	□	[redacted]		Modify Recipient Modify Robot Recipient
Vulnerabilities	□	□	☑	□	[redacted]		Modify Recipient Modify Robot Recipient

f. In the **Operation** column, click **Modify Recipient** or **Modify Robot Recipient** to configure recipients.

   - If you selected email or SMS in **Step 6.e**, configure message recipients.
   - If you selected group chatbots (WeCom, DingTalk, Feishu, and WeLink) in **Step 6.e**, configure robot recipients.

     Only the WeCom, DingTalk, Feishu, and WeLink recipients that have been added on the **Recipient Management** page are available for selection.

g. In the **Modify Recipient** or **Modify Robot Recipient** dialog box, select recipients and click **OK**.

   Only the robot recipients that have been added on the **Recipient Management** page are available for selection. For details about how to add a recipient, see **Adding Recipients**.

- **Use SMN topic settings**

  Select an available topic from the drop-down list or click **View Topics** and create a topic. Alarm notifications are sent to message topic recipients through SMS, chatbots (DingTalk, WeCom, Feishu, and WeLink), and email. For details about message topics, see **Simple Message Notification**.

  To create a topic and add subscriptions, perform the following steps:

  a. Create a topic.

     For details, see **Creating a Topic**.

  b. Add one or more subscriptions to the created topic.

     For details, see **Adding a Subscription**.

  c. After the subscription is added, confirm the subscription as prompted by the received SMS message, email, or other notifications.

The confirmation message about topic subscription may be regarded as spam. If you do not receive the message, check whether it is intercepted as spam.

You can create multiple notification topics based on the O&M plan and alarm notification type to receive different types of alarm notifications.

Step 7 Click **Apply**. A message will be displayed indicating that the alarm notification is set successfully.

----End

Alarm Notifications

Alarm notifications are classified into daily alarm notifications and real-time alarm notifications. The notification items are as follows:

Daily Alarm Notification

The service checks risks in your servers in the early morning every day, summarizes and collects detection results, and sends the results to your mobile phone or email box at 10:00 every day.

Type	Item	Description
Assets	Dangerous ports	Check for high-risk open ports and unnecessary ports.
	Agent not installed	Check for servers with no HSS agent installed, and remind you to install the agent on these servers in a timely manner.
Assets	Dangerous ports	Check for high-risk open ports and unnecessary ports.
	Agent not installed	Check for servers with no HSS agent installed, and remind you to install the agent on these servers in a timely manner.
	Protection interrupted	Check for servers whose agent protection is interrupted, and remind you to rectify faults in a timely manner.
Vulnerabilities	Critical vulnerabilities	Detect critical vulnerabilities and fix them in a timely manner.
Unsafe settings	Unsafe Settings	Detect unsafe settings of key applications that will probably be exploited by hackers to intrude servers.
	Common weak passwords	Detect weak passwords in MySQL, FTP, and system accounts.

Type	Item	Description
Intrusions	Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojans, mining software, worms, and viruses.
	Rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.
	Ransomware	Check for ransomware in media such as web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.
	Web shells	Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. ● Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. ● You can use the manual detection function to detect web shells on servers.
	Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP.
	Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms.
	Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms.
	MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms.
	File privilege escalations	Check the file privilege escalations in your system.
	Process privilege escalations	The following process privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities

Type	Item	Description
	Important file changes	Receive alarms when critical system files are modified.
	File/Directory changes	System files and directories are monitored. If a file or directory is modified, an alarm is generated, indicating that the file or directory may be tampered with.
	Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behaviors. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: ● Abnormal CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections
	High-risk command executions	Check executed commands in real time and generate alarms if high-risk commands are detected.
	Abnormal shells	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.
	Suspicious crontab tasks	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.
	Container image blocking	If a container contains insecure images specified in suspicious image behaviors, an alarm will be generated and the insecure images will be blocked before a container is started in Docker.
	Brute-force attacks	Check for brute-force attack attempts and successful brute-force attacks. ● Detect password cracking attacks on accounts and block attacking IP addresses to prevent server intrusion. ● Trigger an alarm if a user logs in to the server by a brute-force attack.

Type	Item	Description
	Abnormal logins	Check and handle remote logins. If a user's login location is not any common login location you set, an alarm will be triggered.
	Invalid accounts	Scan accounts on servers and list suspicious accounts in a timely manner.
	Vulnerability escapes	The service reports an alarm if it detects container process behavior that matches the behavior of known vulnerabilities (such as Dirty COW, brute-force attack, runC, and shocker).
	File escapes	The service reports an alarm if it detects that a container process accesses a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms.
	Abnormal container processes	Container services are usually simple. If you are sure that only specific processes run in a container, you can add the processes to the whitelist of a policy, and associate the policy with the container. The service reports an alarm if it detects that a process not in the whitelist is running in the container.
	Abnormal container startups	Check for unsafe parameter settings used during container startup. Certain startup parameters specify container permissions. If their settings are inappropriate, they may be exploited by attackers to intrude containers.
	High-risk system calls	Users can run tasks in kernels by Linux system calls. The service reports an alarm if it detects a high-risk call, such as **open_by_handle_at**, **ptrace**, **setns**, and **reboot**.
	Sensitive file access	Detect suspicious access behaviors (such as privilege escalation and persistence) on important files.
	Web page tampering prevention for Windows servers	Protect the static web page files on your Windows website servers from malicious modification.

Type	Item	Description
	Web page tampering prevention for Linux servers	Protect the static web page files on your Linux website servers from malicious modification.
	Dynamic WTP	Protect the dynamic web page files on your Windows and Linux website servers from malicious modification.
	Application protection	Protect running applications. You simply need to add probes to applications, without having to modify application files. Currently, only Linux servers are supported, and only Java applications can be connected.
	Virus scan	Generates alarms for detected virus-infected files.
	Suspicious process executions	Detect and report alarms on unauthenticated or unauthorized application processes.
	Suspicious process file access	Detect and report alarms on the unauthenticated or unauthorized application processes accessing specific directories.

Real-time Alarm Notification

When an event occurs, an alarm notification is immediately sent.

Type	Item	Description
Assets	Dangerous ports	Check for high-risk open ports and unnecessary ports.
	Agent not installed	Check for servers with no HSS agent installed, and remind you to install the agent on these servers in a timely manner.
	Protection interrupted	Check for servers whose agent protection is interrupted, and remind you to rectify faults in a timely manner.
Intrusions	Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojans, mining software, worms, and viruses.
	Rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.

Type	Item	Description
	Ransomware	Check for ransomware in media such as web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.
	Web shells	Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. ● Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. ● You can use the manual detection function to detect web shells on servers.
	Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP.
	Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms.
	Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms.
	MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms.
	File privilege escalations	Check the file privilege escalations in your system.
	Process privilege escalations	The following process privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities
	Important file changes	Receive alarms when critical system files are modified.

Type	Item	Description
	File/Directory changes	System files and directories are monitored. If a file or directory is modified, an alarm is generated, indicating that the file or directory may be tampered with.
	Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behaviors. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: ● Abnormal CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections
	High-risk command executions	Check executed commands in real time and generate alarms if high-risk commands are detected.
	Abnormal shells	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.
	Suspicious crontab tasks	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.
	Container image blocking	If a container contains insecure images specified in suspicious image behaviors, an alarm will be generated and the insecure images will be blocked before a container is started in Docker.
	Abnormal logins	Check and handle remote logins. If a user's login location is not any common login location you set, an alarm will be triggered.
	Invalid accounts	Scan accounts on servers and list suspicious accounts in a timely manner.
	Vulnerability escapes	The service reports an alarm if it detects container process behavior that matches the behavior of known vulnerabilities (such as Dirty COW, brute-force attack, runC, and shocker).

Type	Item	Description
	File escapes	The service reports an alarm if it detects that a container process accesses a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms.
	Abnormal container processes	Container services are usually simple. If you are sure that only specific processes run in a container, you can add the processes to the whitelist of a policy, and associate the policy with the container. The service reports an alarm if it detects that a process not in the whitelist is running in the container.
	Abnormal container startups	Check for unsafe parameter settings used during container startup. Certain startup parameters specify container permissions. If their settings are inappropriate, they may be exploited by attackers to intrude containers.
	High-risk system calls	Users can run tasks in kernels by Linux system calls. The service reports an alarm if it detects a high-risk call, such as **open_by_handle_at**, **ptrace**, **setns**, and **reboot**.
	Sensitive file access	Detect suspicious access behaviors (such as privilege escalation and persistence) on important files.
	Web page tampering prevention for Windows servers	Protect the static web page files on your Windows website servers from malicious modification.
	Web page tampering prevention for Linux servers	Protect the static web page files on your Linux website servers from malicious modification.
	Dynamic WTP	Protect the dynamic web page files on your Windows and Linux website servers from malicious modification.
	Application protection	Protect running applications. You simply need to add probes to applications, without having to modify application files. Currently, only Linux servers are supported, and only Java applications can be connected.

Type	Item	Description
	Auto Blocking	Notify users of successful automatic isolation and killing of malicious programs, automatic blocking of ransomware, and automatic blocking of WTP.
	Suspicious process executions	Detect and report alarms on unauthenticated or unauthorized application processes.
	Suspicious process file access	Detect and report alarms on the unauthenticated or unauthorized application processes accessing specific directories.
Login	Success login	Notifications are sent to accounts that have successfully logged in.
Server protection	Ransomware protection disabled	An alarm is reported if ransomware prevention is disabled manually or abnormally.

2.6 Common Security Configuration

2.6.1 Configuring Server Login Protection

You can configure common login locations, common login IP addresses, and an SSH login IP address whitelist.

Configuring Common Login Locations

A common login location is a geographical location where a user usually uses an account to log in.

HSS continuously monitors the logins of all server accounts, dynamically identifies and adds common login locations, and generates remote login alarms for uncommon login locations. Up to four common login locations can be dynamically added for each server.

After HSS protection is enabled, no alarms will be generated for the location where a user performs the first login. Common login locations include:

- Locations where more than 10 logins occurred.
- Locations where two logins occurred during four consecutive logins.

You can add up to 10 common login locations. HSS will not generate alarms for the logins from these locations.

To view dynamic common login locations and manually add common login locations, perform the following steps:

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

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

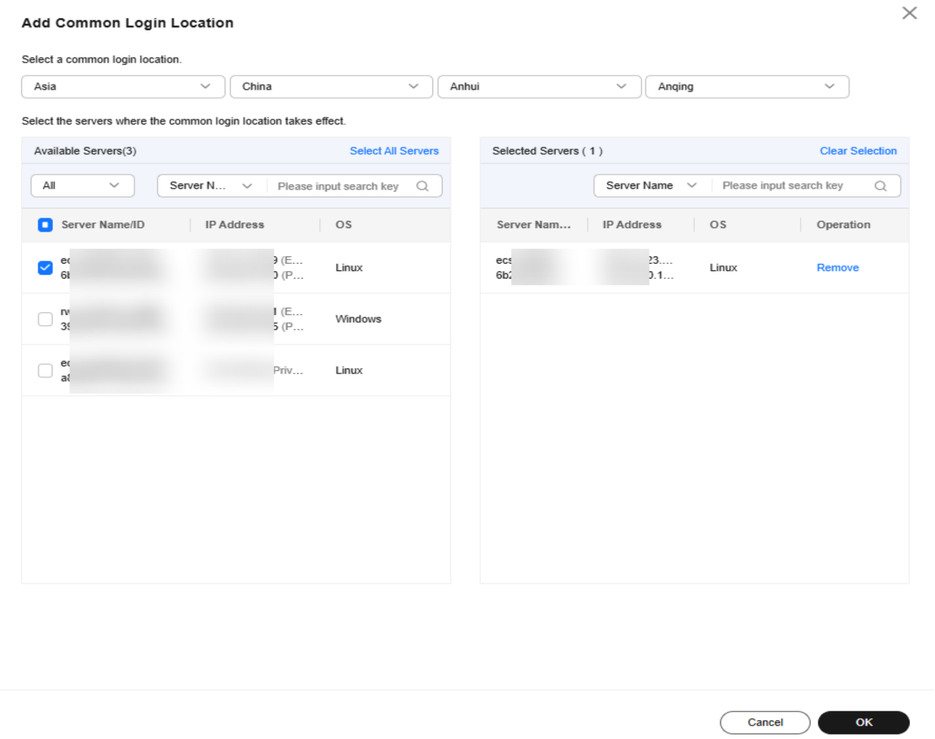
Step 3 Choose **Installation & Configuration** > **Server Install & Config** and click the **Security Configuration** tab. Click **Common Login Locations** and click **Add Common Login Location**.

Step 4 Click **View Dynamic Common Login Locations** to view the common login locations dynamically identified and added by HSS.

Step 5 Click **Add Common Login Location** and manually add locations.

Step 6 In the dialog box that is displayed, select a geographical location and select servers. Confirm the information and click **OK**.

Figure 2-47 Configuring common login locations



Add Common Login Location

Select a common login location.

Asia | China | Anhui | Anqing

Select the servers where the common login location takes effect.

Available Servers(3) — Select All Servers

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

☐ Server Name/ID	IP Address	OS
☑ [redacted]	[redacted]	Linux
☐ [redacted]	[redacted]	Windows
☐ [redacted]	[redacted]	Linux

Selected Servers (1) — Clear Selection

Server Name | Please input search key

Server Nam...	IP Address	OS	Operation
[redacted]	[redacted]	Linux	Remove

Step 7 Return to the **Security Configuration** tab of the **Installation & Configuration** page. Check whether the added locations are displayed on the **Common Login Locations** subtab.

----End

Configuring Common Login IP Addresses

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

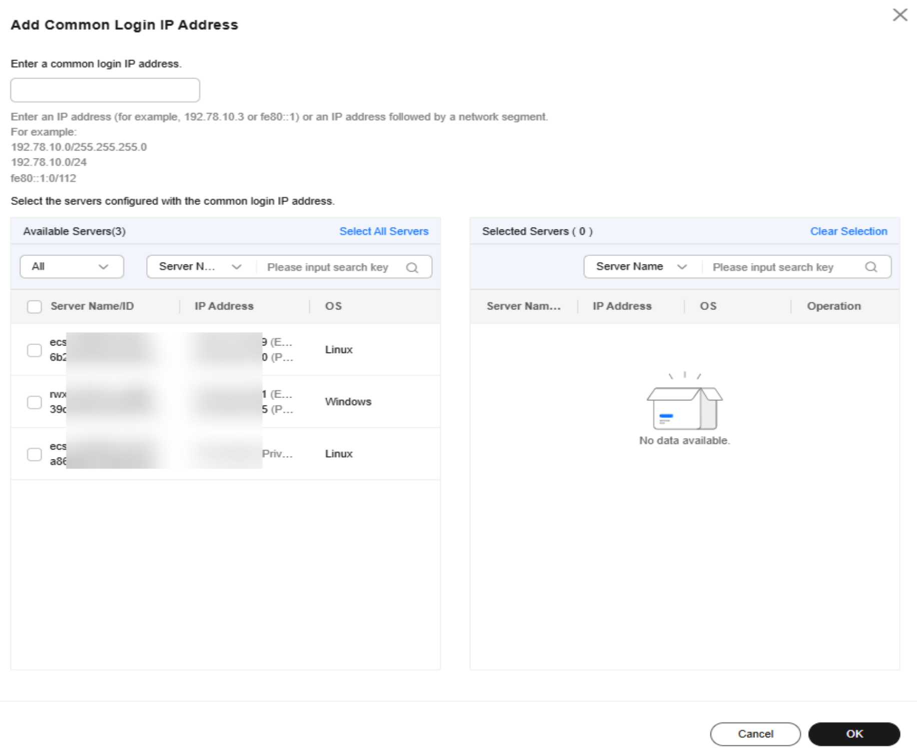
Step 1 Log in to the management console.

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

Step 3 Choose **Installation & Configuration** > **Server Install & Config** and click the **Security Configuration** tab. Click **Common Login IP Addresses** and click **Add Common Login IP Address**.

Step 4 In the dialog box that is displayed, enter a common login IP address and select servers. Confirm the information and click **OK**. For more information, see **Table 2-13**.

Figure 2-48 Entering a common login IP address



Add Common Login IP Address

Enter a common login IP address.

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

Select the servers configured with the common login IP address.

Available Servers(3) Select All Servers

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

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

Selected Servers (0) Clear Selection

Server Name | Please input search key

Server Nam...	IP Address	OS	Operation

No data available.

Table 2-13 Parameters for adding a protected directory

Parameter	Description
Common login IP address	Enter an EIP or CIDR block. If you set non-public IP addresses, you cannot remotely log in to your server using SSH. Example: ● IP address: **192.78.10.3** or **fe80::1** ● CIDR block: **192.78.10.0/255.255.255.0**, **192.78.10.0/24**, or **fe80::1:0/112** Notes: ● You can add only one IP address or CIDR block at a time. To add multiple values, repeat the operation. ● You can add a maximum of 20 login IP addresses.

Parameter	Description
Servers where the common login IP address configuration takes effect	Select the servers where you wish to apply the common login IP addresses. You can select multiple servers at a time.

Step 5 Return to the **Security Configuration** tab of the **Installation & Configuration** page. Check whether the added locations are displayed on the **Common Login IP Addresses** subtab.

----End

Configuring an SSH Login IP Address Whitelist

The SSH login whitelist controls SSH access to servers to prevent account cracking.

- An account can have up to 10 SSH login IP addresses in the whitelist.
- After you configure an SSH login IP address whitelist, SSH logins will be allowed only from the whitelisted IP addresses.
  - Before enabling this function, ensure that all IP addresses that need to initiate SSH logins are added to the whitelist. Otherwise, you cannot remotely log in to your server using SSH.

    If your service needs to access a server, but not necessarily via SSH, you do not need to add its IP address to the whitelist.
  - Exercise caution when adding an IP address to the whitelist. This will make HSS no longer restrict access from this IP address to your servers.

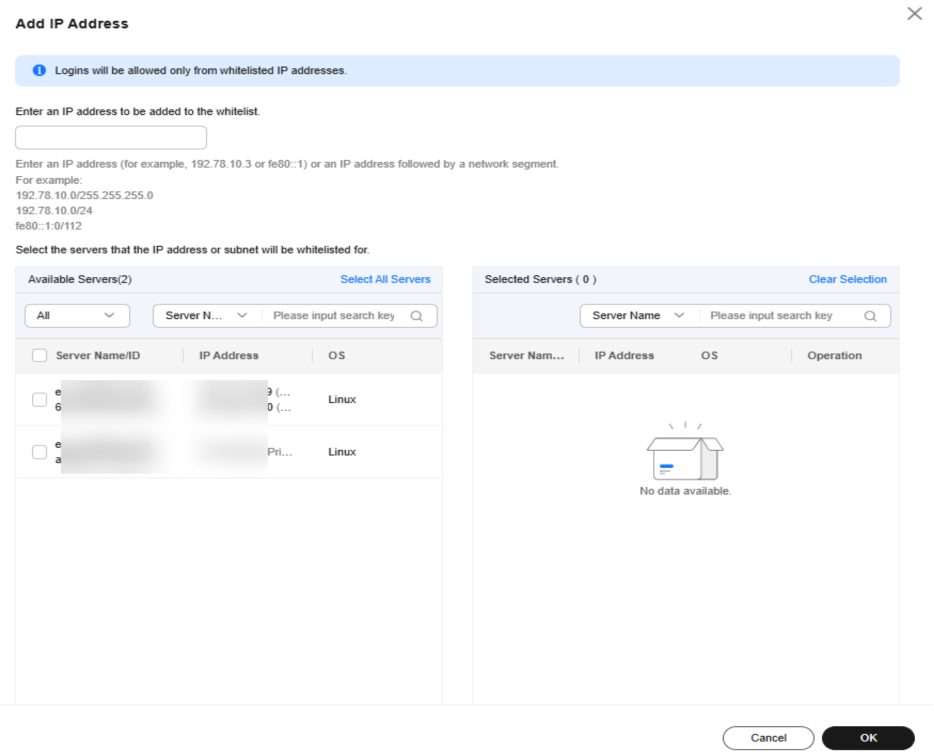
Step 1 Log in to the management console.

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

Step 3 Choose **Installation & Configuration** > **Server Install & Config** and click the **Security Configuration** tab. Click **SSH IP Whitelist** and click **Add IP Address**.

Step 4 In the dialog box that is displayed, enter a whitelisted login IP address and select servers. Confirm the information and click **OK**. For more information, see Table 2-14.

Figure 2-49 Entering an IP address



Add IP Address

Logins will be allowed only from whitelisted IP addresses.

Enter an IP address to be added to the whitelist.

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

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

Available Servers(2) Select All Servers

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

Server Name/ID	IP Address	OS
e 6 [redacted]	[redacted] 9 (... 0 (...	Linux
e a [redacted]	[redacted] Pri...	Linux

Selected Servers (0) Clear Selection

Server Name | Please input search key

Server Nam...	IP Address	OS	Operation

No data available.

Table 2-14 Parameters for adding an SSH login IP address whitelist

Parameter	Description
Whitelisted IP address	Enter an EIP or CIDR block. If you set non-public IP addresses, you cannot remotely log in to your server using SSH. Example: ● IP address: **192.78.10.3** or **fe80::1** ● CIDR block: **192.78.10.0/255.255.255.0**, **192.78.10.0/24**, or **fe80::1:0/112** Notes: ● You can add only one IP address or CIDR block at a time. To add multiple values, repeat the operation. ● You can add up to 10 IP addresses to the whitelist.
Server where the common whitelist IP address configuration takes effect	Select the servers where you wish to apply the whitelisted SSH login IP addresses. You can select multiple servers at a time.

Step 5 Return to the **Security Configuration** tab of the **Installation & Configuration** page. Check whether the added locations are displayed on the **Common Login IP Addresses** subtab.

----End

2.6.2 Isolating and Killing Malicious Programs

HSS automatically isolates and kills identified malicious programs, such as web shells, Trojans, and worms, removing security risks.

Programs are isolated and killed based on their confidence ratings. A high rating indicates a high probability that the detected program is a malicious program. To avoid mistakenly stopping trustworthy programs and affecting services, only the suspicious programs with a high confidence rating are automatically isolated and killed. You can manually isolate and kill programs with lower ratings. For details, see **Handling Server Alarms**.

NOTE

To check the confidence rating of a suspicious program, choose **Detection & Response** > **Alarms** on the HSS console, and click **Server Alarms**. Click a malicious program alarm name to view details.

Isolating and Killing Malicious Programs

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

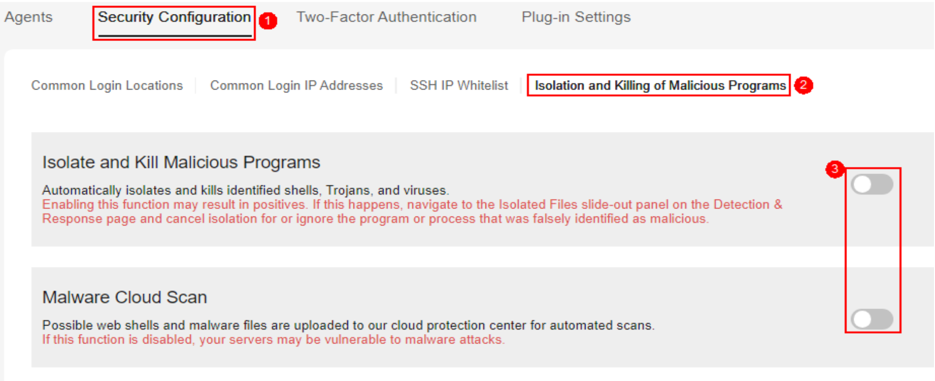
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Installation & Configuration** > **Server Install and Config** and click the **Security Configuration** tab. Click the **Isolation and Killing of Malicious Programs** tab and enable **Isolate and Kill Malicious Programs** and **Malware Cloud Scan**.

NOTE

After the cloud scan function is enabled, all HSS servers will be scanned. Some HSS quota editions can support only limited scanning capabilities. Therefore, you are advised to enable the enterprise edition or higher to enjoy all capabilities of the isolation and killing function.

Figure 2-50 Enabling isolation and killing


Agents
Security Configuration
1
Two-Factor Authentication
Plug-in Settings
Common Login Locations
Common Login IP Addresses
SSH IP Whitelist
Isolation and Killing of Malicious Programs
2
3

Isolate and Kill Malicious Programs

Automatically isolates and kills identified shells, Trojans, and viruses.
Enabling this function may result in positives. If this happens, navigate to the Isolated Files slide-out panel on the Detection & Response page and cancel isolation for or ignore the program or process that was falsely identified as malicious.

Malware Cloud Scan

Possible web shells and malware files are uploaded to our cloud protection center for automated scans.
If this function is disabled, your servers may be vulnerable to malware attacks.

Step 4 In the confirmation dialog box, click **OK** to enable the isolation and killing of malicious programs and malware cloud scan.

Automatic isolation and killing may cause false positives. You can choose **Detection & Response** > **Events** to view isolated malicious programs. You can cancel the isolation or ignore misreported malicious programs. For details, see **Viewing Server Alarms**.

NOTE

- When a program is isolated and killed, the process of the program is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious programs (if any).
- If **Isolate and Kill Malicious Programs** is set to **Disable** on the **Isolation and Killing of Malicious Programs** tab, HSS will generate an alarm when it detects a malicious program.

  To isolate and kill the malicious programs that triggered alarms, choose **Detection & Response** > **Events** and click **Malicious program**.

----End

2.6.3 Enabling and Disabling Agent Self-Protection

Scenario

Agent self-protection can protect HSS software, processes, and files from malicious programs. The protection capabilities vary depending on the OS.

- Self-protection in Windows: Prevents malicious programs from uninstalling the agent, tampering with HSS files, or stopping HSS processes.
- Self-protection in Linux: Prevent malicious programs from stopping HSS processes or uninstalling HSS agents.

This section describes how to enable or disable agent self-protection for the servers protected by the premium or higher edition in an enterprise project.

Comparison Between Agent Self-Protection and the Self-Protection Policy

Agent self-protection and the self-protection policy are the same function, but their application scopes are different. For details, see **Table 2-15**.

Table 2-15 Differences between agent self-protection and the self-protection policy

Function	How to Find	Application Scope and Restriction	Operation
Agent self-protection	**Installation and Configuration** > **Server Install & Config** > **Security Configuration** > **Agent Self-protection**	● After this function is enabled, agent self-protection is enabled for all the servers protected by the premium, container, and WTP editions in the specified enterprise project. ● This switch is displayed only if there is at least one server protected by the premium, container, or WTP edition in the specified enterprise project. ● If the self-protection policy is disabled for a server in the enterprise project, this switch will be displayed as disabled (○).	**Enabling Agent Self-protection** **Disabling Agent Self-protection**
Self-protection policy	**Security Operations** > **Policies** > **policy group of the premium or higher edition (premium, container, or WTP)** > **Self-protection**	After this function is enabled, the agent self-protection function is enabled only for the servers associated with the policy group.	**How Do I Enable or Disable HSS Self-protection?**

Constraints

- Agent self-protection is available only in the HSS premium, WTP, and container editions. It can be used only if the Linux agent version is 3.2.12 or later or the Windows agent version is 4.0.18 or later.
- Agent self-protection in Windows depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled. For details about how to check or enable these functions, see:
  - Ransomware protection: **Enabling Ransomware Prevention**
  - AV detection and HIPS detection: **Configuring Policies**
- Enabling the self-protection policy has the following impacts:
  - **Windows**
    - The agent cannot be uninstalled through the control panel. It can be uninstalled on the HSS console.
    - In the agent installation path **C:\Program Files\HostGuard**, you can only access the **log** and **data** directories (and the **upgrade** directory, if your agent has been upgraded).
    - HSS-related processes cannot be forcibly stopped.
  - **Linux**
    - The agent cannot be uninstalled using commands. It can be uninstalled on the HSS console.
    - If you run a command to stop or restart HSS, you need to enter a verification code, which is displayed in the command output after you run the stop or restart command.
    - HSS-related process information is hidden.

Enabling Agent Self-protection

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

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

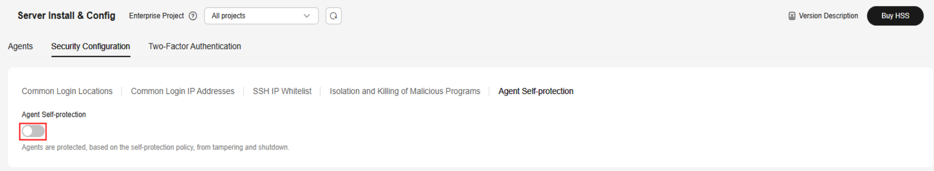
Step 4 Click the **Security Configuration** tab. Click **Agent Self-Protection**.

Step 5 In the upper part of the page, select a project from the **Enterprise Project** drop-down list.

All projects indicates all enterprise projects.

Step 6 Click ○. The **Enable Agent Self-protection?** dialog box is displayed.

Figure 2-51 Agent self-protection



Agents are protected, based on the self-protection policy, from tampering and shutdown.

Step 7 Click **OK**.

indicates that agent self-protection is enabled.

----End

Disabling Agent Self-protection

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**.

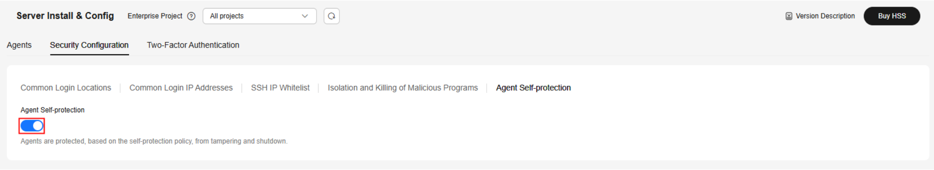
Step 4 Click the **Security Configuration** tab. Click **Agent Self-Protection**.

Step 5 In the upper part of the page, select a project from the **Enterprise Project** drop-down list.

All projects indicates all enterprise projects.

Step 6 Click . The **Disable Agent Self-protection?** dialog box is displayed.

Figure 2-52 Agent self-protection



Agents are protected, based on the self-protection policy, from tampering and shutdown.

Step 7 Click **OK**.

indicates that agent self-protection is disabled.

----End

2.6.4 Enabling 2FA

Two-factor authentication (2FA) requires users to provide verification codes before they log in. The codes will be sent to their mobile phones or email boxes. You have to choose an SMN topic for servers where 2FA is enabled. The topic specifies the recipients of login verification codes, and HSS will authenticate login users accordingly.

Prerequisites

- Server protection has been enabled. For details, see **Enabling Protection**.
- To enable 2FA, you need to disable the SELinux firewall.
- On a Windows server, 2FA may conflict with G01 and 360 Guard (server edition). You are advised to stop them.

Constraints

- If 2FA is enabled, it can be used only in following scenarios:
  - Linux: The SSH password is used to log in to an ECS, and the OpenSSH version is earlier than 8.
  - Windows: The RDP file is used to log in to a Windows ECS.
- When two-factor authentication is enabled for Windows ECSs, the **User must change password at next logon** function is not allowed. To use this function, disable two-factor authentication.

Enabling 2FA

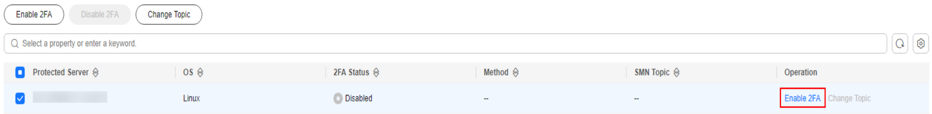
Step 1 **Log in to the management console**.

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

Step 3 Choose **Installation & Configuration** > **Server Install & Config** and click **Two-Factor Authentication**.

Step 4 Select servers and click **Enable 2FA** above the list, or select a server and click **Enable 2FA** in the **Operation** column.

Figure 2-53 Enabling 2FA



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

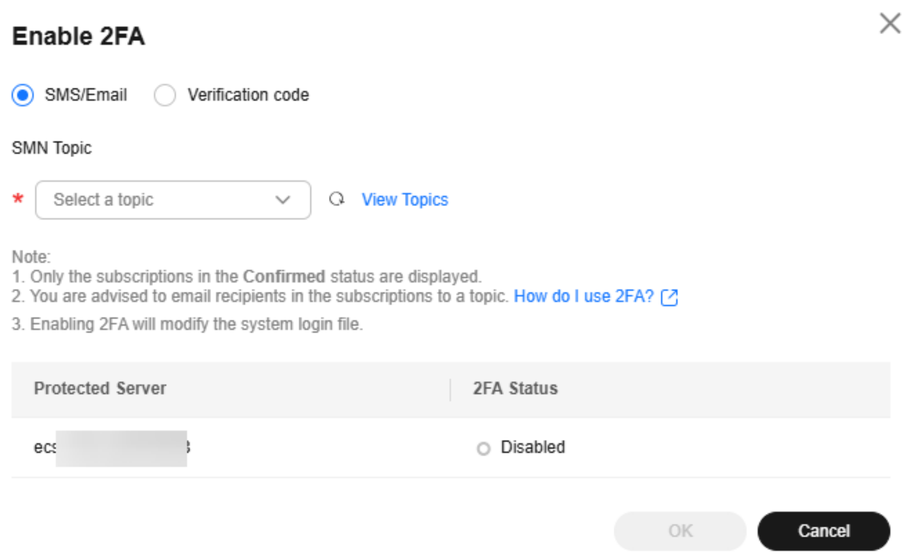
Step 5 In the displayed **Enable 2FA** dialog box, select an authentication mode.

- **SMS/Email**

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

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

Figure 2-54 SMS/Email verification



Enable 2FA

● SMS/Email ○ Verification code

SMN Topic

* Select a topic View Topics

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

Protected Server	2FA Status
ecs[redacted]	○ Disabled

- **Verification code**

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

Step 6 Click **OK**. After 2FA is enabled, it takes about 5 minutes for the configuration to take effect.

When you use a Windows server with 2FA enabled to remotely log in to another Windows server, you need to manually add credentials on the Windows server with 2FA enabled. Otherwise, the remote login will fail.

To add credentials, choose **Start** > **Control Panel**, and click **User Accounts**. Click **Manage your credentials** and then click **Add a Windows credential**. Add the username and password of the remote server that you want to access.

----End

FAQ

- **What Do I Do If I Cannot Enable 2FA?**
- **Why Can't I Receive a Verification Code After 2FA Is Enabled?**
- **How Do I Use 2FA?**

3 Checking the Dashboard

On the HSS dashboard, you can check the security score, risks, and protection overview of all your assets in real time, including servers and containers.

Checking the Dashboard

Step 1 Log in to the management console.

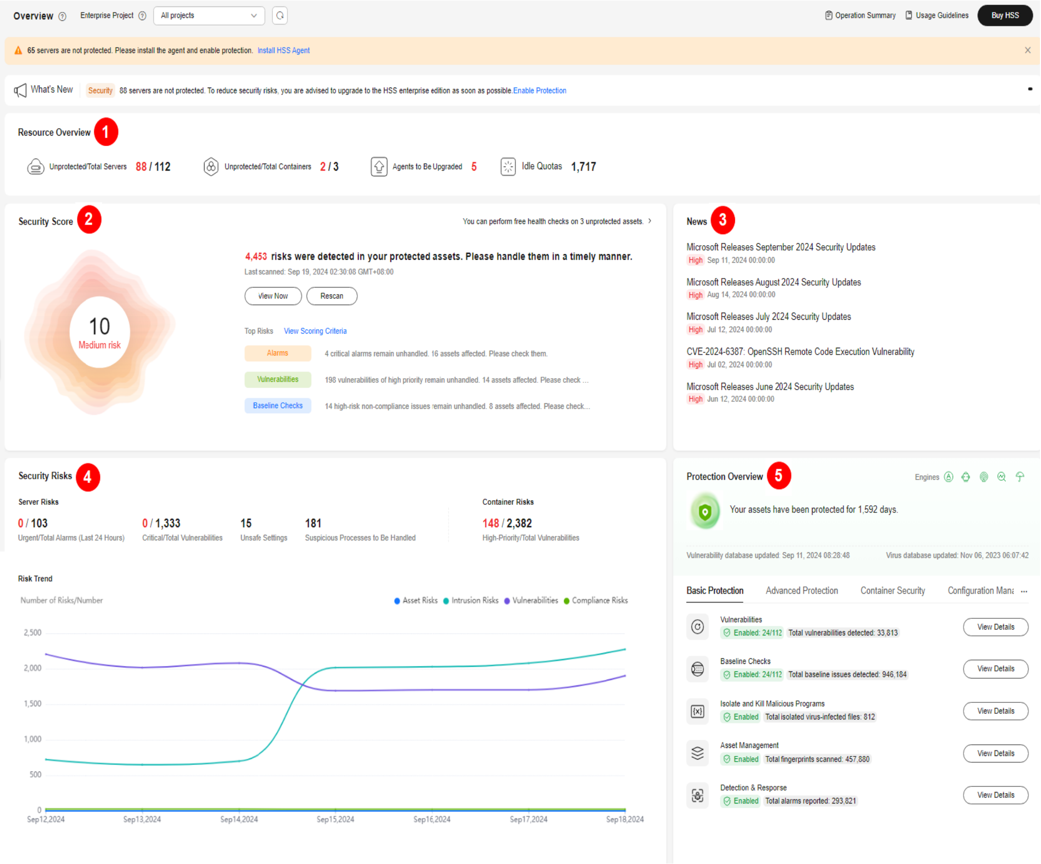
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Overview**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View asset security information. For details, see **Overview information**.

Figure 3-1 Overview



65 servers are not protected. Please install the agent and enable protection. Install HSS Agent

88 servers are not protected. To reduce security risks, you are advised to upgrade to the HSS enterprise edition as soon as possible.Enable Protection

Unprotected/Total Servers 88 / 112

Unprotected/Total Containers 2 / 3

Agents to Be Upgraded 5

Idle Quotas 1,717

You can perform free health checks on 3 unprotected assets.

4,453 risks were detected in your protected assets. Please handle them in a timely manner.

Last scanned: Sep 19, 2024 02:30:08 GMT+08:00

Alarms: 4 critical alarms remain unhandled. 16 assets affected. Please check them.

Vulnerabilities: 198 vulnerabilities of high priority remain unhandled. 14 assets affected. Please check ...

Baseline Checks: 14 high-risk non-compliance issues remain unhandled. 8 assets affected. Please check...

Microsoft Releases September 2024 Security Updates
High Sep 11, 2024 00:00:00

Microsoft Releases August 2024 Security Updates
High Aug 14, 2024 00:00:00

Microsoft Releases July 2024 Security Updates
High Jul 12, 2024 00:00:00

CVE-2024-6387: OpenSSH Remote Code Execution Vulnerability
High Jul 02, 2024 00:00:00

Microsoft Releases June 2024 Security Updates
High Jun 12, 2024 00:00:00

Server Risks

0 / 103 Urgent/Total Alarms (Last 24 Hours)

0 / 1,333 Critical/Total Vulnerabilities

15 Unsafe Settings

181 Suspicious Processes to Be Handled

Container Risks

148 / 2,382 High-Priority/Total Vulnerabilities

Your assets have been protected for 1,592 days.

Vulnerability database updated: Sep 11, 2024 08:28:48

Virus database updated: Nov 06, 2023 06:07:42

Vulnerabilities: Enabled: 24/112 Total vulnerabilities detected: 33,813

Baseline Checks: Enabled: 24/112 Total baseline issues detected: 946,184

Isolate and Kill Malicious Programs: Enabled Total isolated virus-infected files: 812

Asset Management: Enabled Total fingerprints scanned: 457,880

Detection & Response: Enabled Total alarms reported: 293,821

Table 3-1 Overview components

Component	Description
Resource Overview (Component 1 in **Overview**)	Check the percentage of unprotected servers or containers, idle quotas, and agents to be upgraded. ● Click the number of unprotected resources to go to the server or container management page and view the unprotected resource list. ● Click the number of agents to be upgraded to go to the agent list and upgrade agents. ● Click the number of idle quotas to go to the protection quota list. **NOTE** HSS will be continuously upgraded to provide new features and fix bugs. To enjoy better HSS features, upgrade the agent to the latest version in a timely manner. For details, see **Upgrading the agent**.

Component	Description
Secure score (Component 2 in **Overview**)	The security score is in the range 0 to 100. The default score for risk-free assets is 100. Points are deducted based on baseline risks, vulnerability risks, intrusion risks, and asset risks. A low score indicates high security risks in assets. To ensure the security of your assets, you are advised to handle security risks in a timely manner and improve the security score. 1. In the **Security Score** area, click **View Now**. 2. In the **Handle Now** dialog box, view the deduction items and click ⌄ to expand the details. 3. Click **Handle** on the right of deduction items to go to the corresponding risk list. You can rectify the fault based on the risk details and handling suggestions. For details about the score deduction items and how to increase the score, see **Security Scores Criteria and Methods for Improving Scores**. 4. After the risk is fixed, click **Rescan** to update the score.
News (Component 3 in **Overview**)	Latest vulnerability information.

Component	Description
Security risk (Component 4 in **Overview**)	Security risks detected by HSS in your assets. ● **Server Risks** – **Urgent/Total Alarms (Last 24 Hours)**: Number of alarms that need to be handled immediately and the total number of alarms. You can click the number of urgent alarms to go to the **Alarms** page and handle alarms. For details, see **Handling Server Alarms**. – Critical/Total Vulnerabilities: Number of critical vulnerabilities and the total number of vulnerabilities. You can click the number of critical vulnerabilities to go to the **Vulnerabilities** page and handle vulnerabilities. For details, see **Handling Vulnerabilities**. – **Unsafe Settings**: Number of baseline risks to be handled. You can click the number to go to the **Baseline Checks** page and fix baseline risks. For details, see **Viewing and Processing Baseline Check Results**. – **Suspicious Processes to Be Handled**: Total number of suspicious processes to be handled. You can click the number of suspicious processes to be handled to go to the **Application Process Control** page and handle suspicious processes. For details, see **Checking and Handling Suspicious Processes**. ● **Container Risks** **High-Priority/Total Vulnerabilities**: Number of high-risk vulnerabilities and the total number of vulnerabilities. You can click the number of high-priority vulnerabilities to go to the **Image Vulnerabilities** tab and check vulnerability fixing suggestions. ● **Risk Trend** Trends of asset risks, intrusion risks, vulnerability risks, and compliance risks in the last seven days.

Component	Description
Protection overview (Component 5 in **Overview**)	Asset protection overview. ● **Assets**: Total number of assets in the current region. You can click the total number of assets to go to the **Assets** page to view asset distribution and protection status. ● **Unprotected/Total Servers**: Number of unprotected servers and the total number of servers. You can click the number of unprotected servers to go to the **Servers & Quota** page to view servers and enable protection. For details, see **Enabling Protection**. ● **Unprotected/Total Containers**: Number of unprotected containers and the total number of containers. You can click the number of unprotected containers to go to the **Containers & Quota** page to view containers and enable protection. For details, see **Enabling Protection**. ● Vulnerability or virus database update time: The latest update time of the vulnerability or virus database. ● Security feature status: The number of servers protected by each feature and the number of items detected by each feature. You can click **View Details** to go to corresponding feature page.
Best Practices	HSS best practices. Click a title to view details.
FAQ	HSS best FAQ. Click a title to view details.
Related Services	Security services related to HSS. Click a service name to go to its console.

----End

Security Scores Criteria and Methods for Improving Scores

The security score for risk-free assets is 100. A low score indicates high security risks in assets. HSS calculates your security score based on detected security items (vulnerabilities, compliance, intrusions, assets, and images) and unprotected assets. Scores are deducted every time a risk is detected in a category until all scores in that category are deducted. The full score of each category is as follows:

- No vulnerabilities detected: 20. For details about the score deduction criteria and improvement methods, see **Table 3-2**.
- No compliance risks detected: 20. For details about the score deduction criteria and improvement methods, see **Table 3-3**.

- No intrusion risks detected: 30. For details about the score deduction criteria and improvement methods, see **Table 3-4**.
- No asset risks detected: 10. For details about the score deduction criteria and improvement methods, see **Table 3-5**.
- No image risks detected: 10. For details about the score deduction criteria and improvement methods, see **Table 3-6**.
- No unprotected assets detected: 10. For details about the score deduction criteria and improvement methods, see **Table 3-7**.

Table 3-2 Vulnerability risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unhandled vulnerabilities	Unhandled critical vulnerabilities	All	10	√	Fix vulnerabilities based on the suggestions provided, scan for vulnerabilities again, and update the score. ● For details about how to fix vulnerabilities, see **Handling Vulnerabilities**. ● For details about how to scan for vulnerabilities, see **Vulnerability Scan**.
	Unhandled high-risk vulnerabilities	All	3	√	
	Unhandled medium-risk vulnerabilities	All	1	√	
	Unhandled low-risk vulnerabilities	All	0.1	√	

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
No vulnerability scan	No vulnerability scans were performed in the past month.	All	15	×	● The basic edition HSS does not provide vulnerability scan. To use this feature, upgrade HSS to the enterprise or premium edition. For details, see **Upgrading a Protection Quota**. ● In HSS professional, enterprise, premium, and WTP editions, you are advised to perform vulnerability scans. For details, see **Scanning Vulnerabilities**.

Table 3-3 Compliance risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unhandled non-compliance items	Unhandled high-risk non-compliance items	All	10	√	Rectify non-compliance items, perform a baseline check again, and update the score. ● For details about how to fix baseline risks, see **Viewing and Processing Baseline Check Results**. ● For details about how to perform baseline check, see **Performing Baseline Check**.
	Unhandled medium-risk non-compliance items	All	3	√	

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
	Unhandled low-risk non-compliance items	All	1	√	
Weak passwords	Weak passwords	All	10	√	Use strong passwords. For details, see **How Do I Set a Secure Password?**
Weak password check not enabled	Weak password check policy not enabled	All	10	×	Enable the **Weak Password Detection** policy to check for weak passwords on servers. For details, see **Policy Management Overview**.
Baseline check not performed	No baseline checks were performed in the past month.	All	10	×	● The HSS basic and professional editions do not provide baseline check. To use this feature, you are advised to upgrade HSS to the enterprise or premium edition. For details, see **Upgrading a Protection Quota**.

Table 3-4 Intrusion risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unhandled alarms	Critical alarms not fixed	All	10	√	Handle alarms based on the suggestions provided. After alarms are handled, HSS will automatically update the score. For details, see **Handling Server Alarms** and **Handling Container Alarms**.
	Unhandled high-risk alarms	All	3	√	
	Unhandled medium-risk alarms	All	1	√	
	Unhandled low-risk alarms	All	0.1	√	

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Protection not enabled	No security policies enabled	All	30	×	In the HSS professional, enterprise, premium, WTP, and container editions, you need to enable protection policies. For details, see **Policy Management Overview**. The intrusion detection policies that need to be enabled for each edition are as follows: ● Professional/Enterprise edition – Linux: web shell detection, file protection, HIPS detection, login security check, malicious file detection, abnormal process behaviors, root privilege escalation, real-time process, and rootkit detection – Windows: AV detection, web shell detection, HIPS detection, login security check, and real-time process ● Premium/WTP edition – Linux: cluster intrusion detection, web shell detection, file protection, HIPS detection, login security check, malicious file detection, port scan detection, abnormal process behaviors, root

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
					privilege escalation, real-time process, and rootkit detection – Windows: AV detection, web shell detection, HIPS detection, login security check, and real-time process ● Container edition Cluster intrusion detection, container escape detection, web shell detection, container file monitoring, container process whitelist, and suspicious image behaviors
	Login security policy not enabled	All	10	×	In HSS professional, enterprise, premium, WTP, and container editions, you need to enable the **Login Security Check** policy for servers. For details, see **Policy Management Overview**.
	Ransomware prevention policy not enabled	Premium edition	15	×	The HSS premium, WTP, and container editions support ransomware prevention. In these editions, you need to enable the ransomware prevention policy and the backup policy. (10 points will be deducted if backup is not enabled.) For details, see **Enabling Ransomware Prevention**.
	WTP policy is not enabled	WTP edition	20	×	In the HSS WTP edition, you need to enable WTP policy for servers. For details, see **Enabling Protection**.

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
	Container runtime detection policy not enabled	Container edition	20	×	In the HSS container edition, you need to enable container escape, container process whitelist, container file monitoring, and container information collection policies and apply them to servers. For details, see **Overview**.

Table 3-5 Asset risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Open ports	Open TCP/UDP high-risk ports	All	1	√	You are advised to disable unnecessary ports. To enable a port, choose **Asset Management** > **Server Fingerprints**, click **Open Ports**, and ignore the port.

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Asset discovery not enabled	Asset discovery policy not enabled	All	5	×	● The HSS basic, professional, and enterprise editions do not provide asset discovery. To use this feature, upgrade HSS to the premium edition. For details, see **Upgrading a Protection Quota**. ● In the HSS premium and WTP editions, you are advised to enable the **Asset Discovery** policy. For details, see **Policy Management Overview**.

Table 3-6 Image risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Unsafe images	High-risk images	Container edition	3	√	Re-create an image, scan the image, and update the score.
	Medium-risk images	Container edition	1	√	
	Medium-risk images	Container edition	0.1	√	

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Image security scan not performed	No image security scans were performed in the past month.	Container edition	5	×	In the HSS container edition, you are advised to perform image security scans. For details, see: - **Container Image Security**

Table 3-7 Unprotected assets risks score deduction criteria and improvement methods

Category	Score Deduction Item	Affected HSS Edition	Points Deducted	Multiply Deducted Score by Risk Quantity	Methods for Improving Scores
Server protection not enabled	Unprotected servers	All	0.1–1	√	The points deducted for an unprotected server vary depending on its asset importance: - Important asset: 1 - General asset: 0.5 - Test asset: 0.1 You are advised to enable protection for your server as soon as possible. For details, see **Enabling Protection**.

4 Asset Management

4.1 Asset Overview

You can count all your assets and check their statistics, including the agent status, protection status, quota, account, port, process, software, and auto-started items.

Constraints

Servers that are not protected by HSS do not support the asset overview function.

Checking the Asset Overview

Step 1 Log in to the management console.

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

Step 3 Choose **Asset Management** > **Assets**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View assets and their states.

- **Asset Types**: Displays the numbers of servers and container nodes. You can click an asset type in the ring chart to go to the corresponding asset list page.
- **Agent Status**: Displays the number of servers in the **Online**, **Offline**, and **Not installed** states. You can click an agent status in the ring chart to go to the corresponding server list page.
- **Servers**: Displays the number of unprotected and protected servers. You can click a server type in the ring chart to go to the corresponding server list page. For details about how to enable protection, see **Enabling Protection**.
- **Containers**: Displays the number of unprotected and protected container nodes. You can click a container type in the ring chart to go to the corresponding container node list page. For details about how to enable protection, see **Enabling Protection**.

- **Quotas**: Displays the protected quota types and their usage status. You can click **Protected Servers** or **Protected Containers** to go to the corresponding protected quota list page.
- **OS Types**: Displays the number and proportion of OS types. You can click an OS type in the ring chart to go to the corresponding server list page.
- **Asset Counting**: Displays asset information, including account information, open ports, processes, installed software, auto-startup items, web applications, web services, web frameworks, websites, middleware, databases, and kernel modules. You can click the value of each asset item to go to the corresponding asset list page.

----End

4.2 Server Fingerprints

4.2.1 Collecting Server Asset Fingerprints

Scenarios

HSS can collect server fingerprints, including information about ports, processes, web applications, web services, web frameworks, and auto-started items. You can centrally check server information and detect risky assets in a timely manner based on the server fingerprints. This section describes server asset fingerprints and their collection method.

Constraints

The server fingerprint function is available in HSS enterprise, premium, WTP, and container editions. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.

Server Fingerprint Collection Items

Server fingerprints: accounts, open ports, processes, software, auto-started items, web applications, web services, web frameworks, websites, middleware, kernel modules, and databases. For details, see **Server Fingerprint Collection Items**.

Table 4-1 Server fingerprint collection items

Item	Description	Supported OS
Accounts	Check and manage all accounts on your servers to keep them secure. You can check real-time and historical account information to find suspicious accounts. ● Real-time account information includes the account name, number of servers, server name/IP address, login permission, root permission, user group, user directory, shell started by the user, the last scan time, and the first scan time. ● Historical account change records include the server name/IP address, change status, login permission, root permission, user group, user directory, shell started by the user, and the last scan time.	Linux and Windows
Open ports	Check open ports on your servers, including risky and unknown ports. You can easily identify high-risk ports by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files. ● Manually disabling high-risk ports If dangerous or unnecessary ports are found enabled, check whether they are mandatory for services, and disable them if they are not. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary. It is recommended that you handle the ports at the **Dangerous** risk level promptly and handle the ports at the **Unknown** risk level based on the actual service conditions. ● Ignore risks: If a detected high-risk port is actually a normal port used for services, you can ignore it. The port will no longer be regarded risky or generate alarms.	Linux and Windows
Processes	Check processes on your servers and find abnormal processes. You can easily identify abnormal processes based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes. If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.	Linux and Windows

Item	Description	Supported OS
Installed software	Check and manage all software installed on your containers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. ● Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, the last scan time, and the first scan time. ● Historical software change records include the server names, IP addresses, change statuses, software versions, software update time, and the last scan time.	Linux and Windows
Auto-started items	Check for auto-startup items and quickly locate Trojans. ● Real-time information about auto-started items includes their names, types (auto-started service, startup folder, pre-loaded dynamic library, Run registry key, or scheduled task), number of servers, server names, IP addresses, paths, file hashes, users, and the last scan time. ● The historical change records of auto-started items include server names, IP addresses, change statuses, paths, file hashes, users, and the last scan time.	Linux and Windows
Websites	Check information about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, certificate information (to be provided later), and key processes of websites. Information about the following websites can be collected: Linux-based Apache, Nginx, and Tomcat.	Linux

Item	Description	Supported OS
Web frameworks	Check information about frameworks used for web content display, including their versions, paths, and associated processes. The following types of web frameworks based on Linux support data collection: ● Java language framework: Struts, struts2, spring, hibernate, webwork, quartz, velocity, turbine, FreeMarker, flexive, stripes, vaadin, vertx, wicket, zkoss, jackson, fastjson, shiro, MyBatis, Jersey and JFinal. ● Python framework: Django, Flask, Tornado, web.py, and web2py. ● PHP language framework: Webasyst, KYPHP, CodeIgniter, InitPHP, SpeedPHP, ThinkPHP, and OneThink ● Go framework: Gin, Beego, Fasthttp, Iris, and Echo.	Linux
Middleware	Check information about servers, versions, paths, and processes associated with middleware.	Linux and Windows
Kernel module	Check information about all the program module files running in kernels, including associated servers, version numbers, module descriptions, driver file paths, file permissions, and file hashes.	Linux
Web services	Check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software. The following types of web services support data collection: ● Linux: Apache, Nginx, Tomcat, Weblogic, WebSphere, JBoss, Wildfly, and Jetty ● Windows: Tomcat	Linux and Windows
Web applications	Check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software. The following types of web applications support data collection: ● Linux: PHPMailer, PHPMyadmin, DedeCMS, WordPress, ThinkPHP, BigTree, JPress, Jenkins, Zabbix, Discuz!, and ThinkCMF. ● Windows: Chanjet	Linux and Windows

Item	Description	Supported OS
Databases	Check details about the software that provides data storage, including versions, paths, configuration files, and associated processes of all software. Information about the following types of databases can be collected: ● Linux: MySQL, Redis, Oracle, MongoDB, Memcache, PostgreSQL, HBase, DB2, Sybase, Dameng database management system, and KingbaseES database management system. ● Windows: MySQL	Linux and Windows

Server Fingerprint Collection Modes

Server fingerprints can be collected automatically or manually. For details about how each type of fingerprints is collected, see **Table 4-2**.

After the agent is installed on a server, the fingerprints of the server will be collected for the first time immediately. By default, the automatic collection period starts from the time when the agent installation succeeded.

If you are using the HSS premium edition or higher, you can customize the interval for automatically collecting data of middleware, web frameworks, kernel modules, web applications, websites, web services, and databases. For details, see **Asset Discovery**.

Table 4-2 Server fingerprint collection modes

Item	Automatic Check Frequency	Manual Collection Method
Accounts	Automatic check every hour	See **Manually Collecting the Latest Asset Fingerprints of All Servers**.
Open ports	Automatic check every 30 seconds	See **Manually Collecting the Latest Asset Fingerprints of All Servers**.
Processes	Automatic check every hour	See **Manually Collecting the Latest Asset Fingerprints of All Servers**.

Item	Automatic Check Frequency	Manual Collection Method
Installed software	Automatic check every day	See **Manually Collecting the Latest Asset Fingerprints of All Servers**.
Auto-started items	Automatic check every hour	See **Manually Collecting the Latest Asset Fingerprints of All Servers**.
Websites	Once a week (04:10 a.m. every Monday)	See **Manually Collecting the Latest Asset Fingerprints of All Servers** and **Manually Collecting the Latest Asset Fingerprints of a Single Server**.
Web frameworks	Once a week (04:10 a.m. every Monday)	See **Manually Collecting the Latest Asset Fingerprints of All Servers** and **Manually Collecting the Latest Asset Fingerprints of a Single Server**.
Middleware	Once a week (04:10 a.m. every Monday)	See **Manually Collecting the Latest Asset Fingerprints of All Servers** and **Manually Collecting the Latest Asset Fingerprints of a Single Server**.
Kernel module	Once a week (04:10 a.m. every Monday)	See **Manually Collecting the Latest Asset Fingerprints of All Servers** and **Manually Collecting the Latest Asset Fingerprints of a Single Server**.
Web services	Once a week (04:10 a.m. every Monday)	See **Manually Collecting the Latest Asset Fingerprints of All Servers** and **Manually Collecting the Latest Asset Fingerprints of a Single Server**.

Item	Automatic Check Frequency	Manual Collection Method
Web applications	Once a week (04:10 a.m. every Monday)	See **Manually Collecting the Latest Asset Fingerprints of All Servers** and **Manually Collecting the Latest Asset Fingerprints of a Single Server**.
Databases	Once a week (04:10 a.m. every Monday)	See **Manually Collecting the Latest Asset Fingerprints of All Servers** and **Manually Collecting the Latest Asset Fingerprints of a Single Server**.

Manually Collecting the Latest Asset Fingerprints of a Single Server

If you want to obtain the latest data of assets such as web applications, web services, web frameworks, websites, middleware, kernel modules, and databases in real time, you can manually collect fingerprint information.

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

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

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

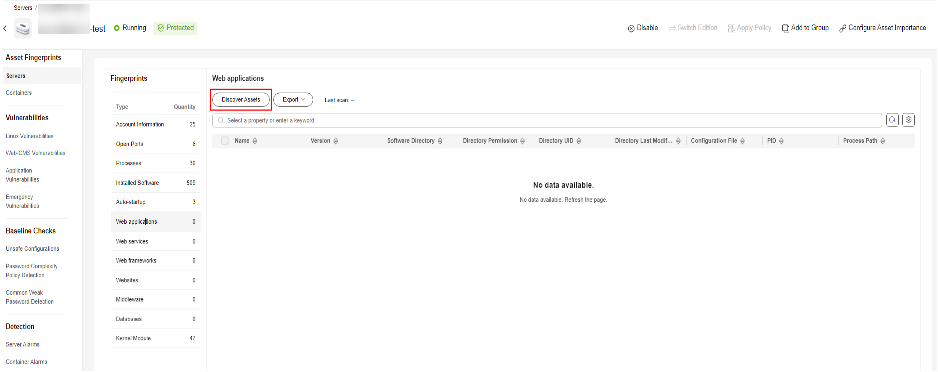
Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Servers**.

Step 6 Click a fingerprint in the fingerprint list, and click **Discover Assets** on the upper area of the list on the right.

Currently, only the information about web applications, web services, web frameworks, websites, middleware, kernel modules, and databases can be manually collected and updated in real time. Information about other types is automatically collected and updated every day.

Figure 4-1 Collecting data now



Type	Quantity
Account Information	25
Open Ports	6
Processes	30
Installed Software	509
Auto-startup	3
Web applications	0
Web services	0
Web frameworks	0
Websites	0
Middleware	0
Databases	0
Kernel Module	47

Name	Version	Software Directory	Directory Permission	Directory UID	Directory Last Modif...	Configuration File	PID	Process Path

No data available.

No data available. Refresh the page.

Step 7 After the automatic execution is complete, the last scan time is updated and the latest server asset information is displayed.

----End

Manually Collecting the Latest Asset Fingerprints of All Servers

To view the latest fingerprints of all server assets in real time, you can manually collect fingerprints.

Step 1 Log in to the management console.

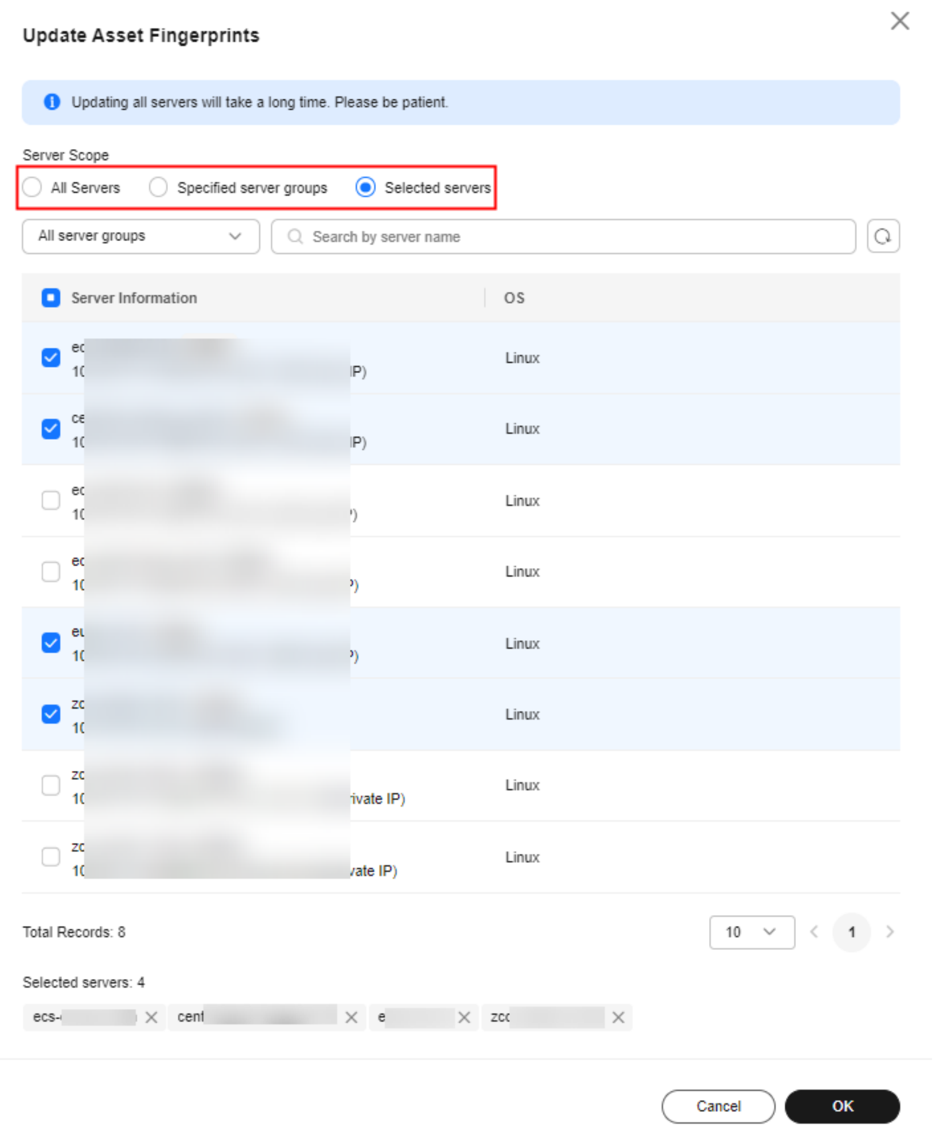
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Asset Management** > **Server Fingerprints**.

Step 4 In the upper right corner of the page, click **Update Asset Fingerprints**.

Step 5 Select the server update scope and click **OK**.

Figure 4-2 Updating asset fingerprints



Update Asset Fingerprints

Updating all servers will take a long time. Please be patient.

Server Scope

○ All Servers ○ Specified server groups ● Selected servers

■ Server Information	OS
☑ ec [redacted] 10 [redacted] IP)	Linux
☑ ce [redacted] 10 [redacted] IP)	Linux
□ ec [redacted] 10 [redacted])	Linux
□ ec [redacted] 10 [redacted])	Linux
☑ eu [redacted] 10 [redacted])	Linux
☑ zc [redacted] 10 [redacted]	Linux
□ zc [redacted] 10 [redacted] ivate IP)	Linux
□ zc [redacted] 10 [redacted] vate IP)	Linux

Total Records: 8

Selected servers: 4

ecs- [redacted] × cent [redacted] × e [redacted] × zc([redacted] ×

Step 6 After the **Updating Asset Fingerprints** status disappears from the button in the upper right corner of the page, you can view the latest asset fingerprints.

----End

Follow-up Procedure

After the server fingerprints are collected, you can view the latest asset fingerprint data. For details, see **Viewing Server Asset Fingerprints**.

4.2.2 Viewing Server Asset Fingerprints

HSS can collect server asset fingerprints, including information about ports, processes, web applications, web services, web frameworks, and auto-started items. You can centrally check server asset information and detect risky assets in a timely manner based on the server fingerprints.

This section describes how to view the collected server asset fingerprints on the console. For more information, see **Collecting Server Asset Fingerprints**.

Constraints

The server fingerprint function is available in HSS enterprise, premium, WTP, and container editions. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.

Viewing Asset Information of All Servers

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

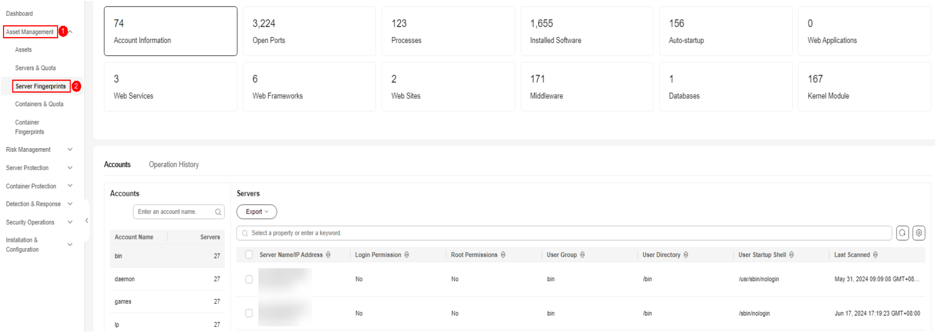
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Asset Management** > **Server Fingerprints**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View the server fingerprints.

Figure 4-3 Viewing server fingerprints



74 Account Information	3,224 Open Ports	123 Processes	1,655 Installed Software	156 Auto-startup	0 Web Applications
3 Web Services	6 Web Frameworks	2 Web Sites	171 Middleware	1 Databases	167 Kernel Module

Accounts

Account Name	Servers
bin	27
daemon	27
games	27
lp	27

Servers

Server Name/IP Address	Login Permission	Root Permissions	User Group	User Directory	User Startup Shell	Last Scanned
[redacted]	No	No	bin	/bin	/usr/sbin/nologin	May 31, 2024 09:09:08 GMT+08...
[redacted]	No	No	bin	/bin	/sbin/nologin	Jun 17, 2024 17:19:23 GMT+08:00

Step 6 Click a fingerprint type in the list to view the asset information.

Step 7 (Optional) Remove risky assets.

If you find unsafe assets after counting, remove them in a timely manner.

If you receive port alarms, you can set **Dangerous Port** to **Yes** in the search box of the **Open Ports** area to filter dangerous ports. You are advised to handle unsafe ports as follows:

- If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. If they are not, disable them. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.
- If a detected high-risk port is actually a normal port used for services, you can ignore it. Ignored alarms will neither be recorded as unsafe items and nor trigger alarms.

For more information, see **High-risk port list**.

----End

Viewing the Asset Information of a Single Server

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

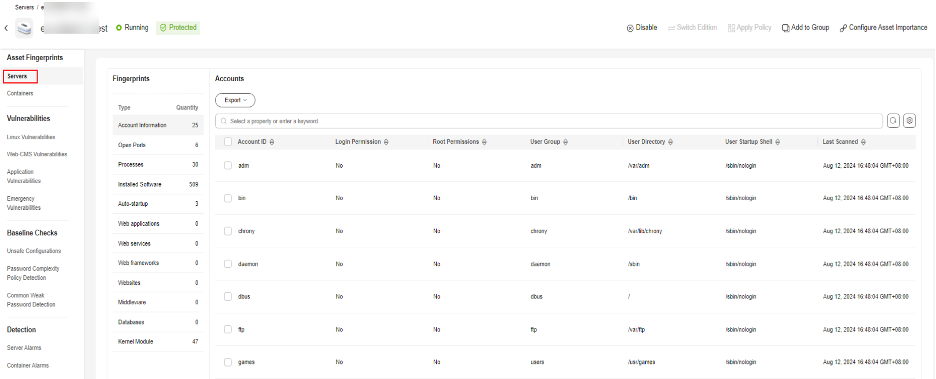
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Servers**.

Figure 4-4 Viewing asset fingerprints of a single server



Type	Quantity
Account Information	25
Open Ports	6
Processes	30
Installed Software	509
Auto-startup	3
Web applications	0
Web services	0
Web frameworks	0
Websites	0
Middleware	0
Databases	0
Kernel Module	47

Account ID	Login Permission	Root Permissions	User Group	User Directory	User Startup Shell	Last Scanned
adm	No	No	adm	/var/adm	/sbin/nologin	Aug 12, 2024 16:48:04 GMT+08:00
bin	No	No	bin	/bin	/sbin/nologin	Aug 12, 2024 16:48:04 GMT+08:00
chrony	No	No	chrony	/var/lib/chrony	/sbin/nologin	Aug 12, 2024 16:48:04 GMT+08:00
daemon	No	No	daemon	/sbin	/sbin/nologin	Aug 12, 2024 16:48:04 GMT+08:00
dbus	No	No	dbus	/	/sbin/nologin	Aug 12, 2024 16:48:04 GMT+08:00
ftp	No	No	ftp	/var/ftp	/sbin/nologin	Aug 12, 2024 16:48:04 GMT+08:00
games	No	No	users	/usr/games	/sbin/nologin	Aug 12, 2024 16:48:04 GMT+08:00

Step 6 Click a fingerprint type in the list to view the asset information.

Step 7 (Optional) Remove risky assets.

If you find unsafe assets after counting, remove them in a timely manner.

If you receive port alarms, you can set **Dangerous Port** to **Yes** in the search box of the **Open Ports** area to filter dangerous ports. You are advised to handle unsafe ports as follows:

- If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. If they are not, disable them. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.
- If a detected high-risk port is actually a normal port used for services, you can ignore it. Ignored alarms will neither be recorded as unsafe items and nor trigger alarms.

For more information, see **High-risk port list**.

----End

High-risk port list

Table 4-3 lists the high-risk ports are identified by the asset fingerprint function of HSS. If a high-risk port is enabled in your asset, check whether they are really used by your services.

Table 4-3 High-risk port list

Port	Description	Protocol
31	Trojan horses Master Paradise and Hackers Paradise	TCP and UDP
456	Trojan horses HACKERSPARADISE	TCP and UDP
555	Trojan horses PhAse1.0 Stealth Spy and IniKiller	TCP and UDP
666	Trojan horses Attack FTP and Satanz Backdoor	TCP and UDP
1001	Trojan horses Silencer and WebEx	TCP and UDP
1011	Doly Trojan	TCP and UDP
1025	Trojan netspy	TCP and UDP
1033	Trojan netspy	TCP and UDP
1070	Trojan horses Streaming Audio Trojan, Psyber Stream Server, and Voice	TCP and UDP
1234	Trojan horses SubSeven2.0 and Ultors Trojan	TCP and UDP
1243	Trojan SubSeven 1.0/1.9	TCP and UDP
1245	Trojan Voodoo	TCP and UDP
1270	MOM-Encrypted Microsoft Operations Manager (MOM)	TCP
1492	Trojan FTP99CMP	TCP and UDP
1600	Trojan Shivka-Burka	TCP and UDP
1807	Trojan SpySender	TCP and UDP
1981	Trojan ShockRave	TCP and UDP
1999	Trojan BackDoor	TCP and UDP
2000	Trojans GirlFriend 1.3 and Millenium 1.0	TCP and UDP
2001	Trojan Millenium 1.0 and Trojan Cow	TCP and UDP
2023	Trojan Pass Ripper	TCP and UDP

Port	Description	Protocol
2115	Trojan Bugs	TCP and UDP
2140	Trojan Deep Throat 1.0/3.0	TCP and UDP
3150	Trojan Deep Throat 1.0/3.0	TCP and UDP
6711	Trojan SubSeven1.0/1.9	TCP and UDP
6776	Trojan horses SubSeven2.0 and Ultors Trojan and SubSeven1.0/1.9	TCP and UDP

4.2.3 Viewing the Operation History of Server Assets

HSS proactively records the changes on account information, software information, and auto-started items. You can check the change details according to different dimensions and time ranges.

Constraints

The server fingerprint function is available in HSS enterprise, premium, WTP, and container editions. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.

Checking Change Records

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

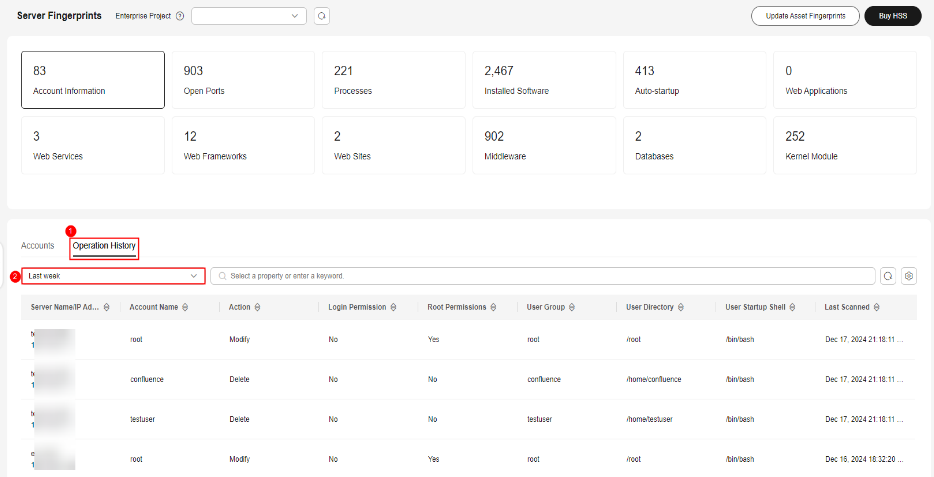
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Asset Management** > **Server Fingerprints** and click the **Operation History** tab page.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Select a dimension and a time range to view the historical changes of accounts, software, and auto-started items. For details about the changes in accounts, software, and auto-started items, see **Table 4-4**.

Figure 4-5 Operation history of server assets



83 Account Information
903 Open Ports
221 Processes
2,467 Installed Software
413 Auto-startup
0 Web Applications
3 Web Services
12 Web Frameworks
2 Web Sites
902 Middleware
2 Databases
252 Kernel Module

Last week

Server Name/IP Ad...	Account Name	Action	Login Permission	Root Permissions	User Group	User Directory	User Startup Shell	Last Scanned
[redacted]	root	Modify	No	Yes	root	/root	/bin/bash	Dec 17, 2024 21:18:11 ...
[redacted]	confluence	Delete	No	No	confluence	/home/confluence	/bin/bash	Dec 17, 2024 21:18:11 ...
[redacted]	testuser	Delete	No	No	testuser	/home/testuser	/bin/bash	Dec 17, 2024 21:18:11 ...
[redacted]	root	Modify	No	Yes	root	/root	/bin/bash	Dec 16, 2024 18:32:20 ...

Table 4-4 Description of change history

Asset Type	Change History
Account	Records changes such as account creation and deletion; and modification of account names, administrator rights, and user groups.
Software	Records added and deleted software.
Auto-started item	Records new auto-started items and changes in their running periods, attributes, hashes, and paths.

----End

4.3 Container Assets

4.3.1 Collecting Container Assets

Scenarios

HSS can collect information about container assets, including clusters, nodes, containers, images, and container fingerprints. With the container asset function, you can centrally count container assets and detect unsafe assets in a timely manner. This section describes the container asset collection items and how they are collected.

Prerequisite

Container assets have been connected to HSS. For details, see **Connecting to a Third-party Image Repository**, **Accessing CI/CD**, and **Installing an Agent in a Cluster**.

Constraints

The container fingerprint function is supported only by the HSS enterprise edition. For details about how to purchase HSS, see **Purchasing an HSS Quota**.

Container Asset Collection Items

The container asset function can collect information about container assets, including clusters, nodes, containers, images, and container fingerprints. Container fingerprints are classified into multiple subtypes, including accounts, open ports, processes, software, auto-started items, web applications, web services, web frameworks, websites, middleware, and databases. For details about assets, see **Table 4-5**.

Table 4-5 Container asset collection items

Item	Description
Clusters	You can check statistics and details about clusters, workloads, services, and pods.
Nodes	You can check details about cluster nodes and independent nodes.
Containers	You can check details about container instances.
Images	You can check information about local images, repository images, and CI/CD images.
Accounts	Check and manage all accounts on your containers to keep them secure. Real-time account information includes the account name, number of servers, server name, IP address, login permission, root permission, user group, user directory, shell started by the user, container name, container ID, the last scan time, and the first scan time.

Item	Description
Open ports	Check open ports on your containers, including risky and unknown ports. You can easily find high-risk ports on containers by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files. ● Manually disabling high-risk ports If dangerous or unnecessary ports are found enabled, check whether they are mandatory for services, and disable them if they are not. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary. It is recommended that you handle the ports with the **Dangerous** risk level promptly and handle the ports with the **Unknown** risk level based on the actual service conditions. ● Ignore risks: If a detected high-risk port is actually a normal port used for services, you can ignore it. The port will no longer be regarded risky or generate alarms.
Processes	Check processes on your containers and find abnormal processes. You can easily identify abnormal processes on your containers based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes. If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.
Installed software	Check and manage all software installed on your containers, and identify insecure versions. You can check real-time and historical software information to determine whether the software is risky. ● Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, the last scan time, and the first scan time. ● Historical software change records include the server names, IP addresses, change statuses, software versions, software update time, and the last scan time.
Auto-started items	Check for auto-started items and quickly locate Trojans. Real-time information about auto-started items includes their names, types (auto-started service, startup folder, pre-loaded dynamic library, Run registry key, or scheduled task), number of servers, server names, IP addresses, paths, file hashes, users, container name, container ID, and the last scan time.

Item	Description
Websites	Check information about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, certificate information (to be provided later), and key processes of websites. The following websites support data collection: Apache, Nginx, and Tomcat.
Web frameworks	Check statistics about frameworks used for web content display, including their versions, paths, and associated processes. The following types of web frameworks support data collection: ● Java language framework: Struts, struts2, spring, hibernate, webwork, quartz, velocity, turbine, FreeMarker, flexive, stripes, vaadin, vertx, wicket, zkoss, jackson, fastjson, shiro, MyBatis, Jersey and JFinal. ● Python framework: Django, Flask, Tornado, web.py, and web2py. ● PHP language framework: Webasyst, KYPHP, CodeIgniter, InitPHP, SpeedPHP, ThinkPHP, and OneThink ● Go framework: Gin, Beego, Fasthttp, Iris, and Echo.
Middleware	Check information about servers, versions, paths, and processes associated with middleware.
Web services	Check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software. Data can be collected from the following web services: Apache, Nginx, Tomcat, WebLogic, WebSphere, JBoss, Wildfly, and Jetty.
Web applications	Check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software. Data of the following web applications can be collected: PHPMailer, PHPMyadmin, DedeCMS, WordPress, ThinkPHP, BigTree, JPress, Jenkins, Zabbix, Discuz!, and ThinkCMF.
Databases	Check details about the software that provides data storage, including versions, paths, configuration files, and associated processes of all software. Data can be collected from the following types of databases: MySQL, Redis, Oracle, MongoDB, Memcache, PostgreSQL, HBase, DB2, Sybase, Dameng database management system, and KingbaseES database management system.

Container Asset Collection Methods

Container asset information can be collected automatically or manually. For details about how each type of fingerprints is collected, see **Table 4-6**.

After the agent is installed on a cluster node or independent node, information about server assets will be collected for the first time immediately. By default, the automatic collection period starts from the time when the agent installation succeeded.

Collection intervals can be customized for middleware, web frameworks, kernel modules, web applications, websites, web services, and databases. For details, see **Asset Discovery**.

Table 4-6 Container asset collection methods

Item	Automatic Collection Frequency	Manual Collection Method
Clusters	Automatic check every 24 hours	See **Manually Collecting Cluster, Service, Workload, and Container Information**.
Nodes	● Cluster nodes: automatic check every 24 hours ● Independent nodes: Data is automatically collected after the agent is installed.	None
Containers	Automatic check every 24 hours	See **Manually Collecting Cluster, Service, Workload, and Container Information**.
Images	● Local images: – Images on cluster nodes: automatic check every 24 hours – Images on independent nodes: Data is automatically collected after the agent is installed. ● Repository image: None. Manual collection required. ● CI/CD image: Data is automatically collected during CI/CD project building.	● Local image and CI/CD image: Data cannot be collected manually. ● For details about how to manually collect repository images, see **Synchronizing Repository Images**.
Accounts	Automatic check every hour	See **Manually Collecting the Latest Asset Fingerprints of All Containers**.
Open ports	Automatic check every 30 seconds	See **Manually Collecting the Latest Asset Fingerprints of All Containers**.

Item	Automatic Collection Frequency	Manual Collection Method
Processes	Automatic check every hour	See **Manually Collecting the Latest Asset Fingerprints of All Containers**.
Installed software	Automatic check every day	See **Manually Collecting the Latest Asset Fingerprints of All Containers**.
Auto-started items	Automatic check every hour	See **Manually Collecting the Latest Asset Fingerprints of All Containers**.
Websites	Once a week (04:10 a.m. every Monday)	For details, see **Manually Collecting the Latest Asset Fingerprints of a Single Container** or **Manually Collecting the Latest Asset Fingerprints of All Containers**.
Web frameworks	Once a week (04:10 a.m. every Monday)	For details, see **Manually Collecting the Latest Asset Fingerprints of a Single Container** or **Manually Collecting the Latest Asset Fingerprints of All Containers**.
Middleware	Once a week (04:10 a.m. every Monday)	For details, see **Manually Collecting the Latest Asset Fingerprints of a Single Container** or **Manually Collecting the Latest Asset Fingerprints of All Containers**.
Web services	Once a week (04:10 a.m. every Monday)	For details, see **Manually Collecting the Latest Asset Fingerprints of a Single Container** or **Manually Collecting the Latest Asset Fingerprints of All Containers**.

Item	Automatic Collection Frequency	Manual Collection Method
Web applications	Once a week (04:10 a.m. every Monday)	For details, see **Manually Collecting the Latest Asset Fingerprints of a Single Container** or **Manually Collecting the Latest Asset Fingerprints of All Containers**.
Databases	Once a week (04:10 a.m. every Monday)	For details, see **Manually Collecting the Latest Asset Fingerprints of a Single Container** or **Manually Collecting the Latest Asset Fingerprints of All Containers**.

Manually Collecting the Latest Asset Fingerprints of a Single Container

To view the latest data of web applications, web services, web frameworks, websites, middleware, and databases in real time, you can manually collect their fingerprints.

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

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

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

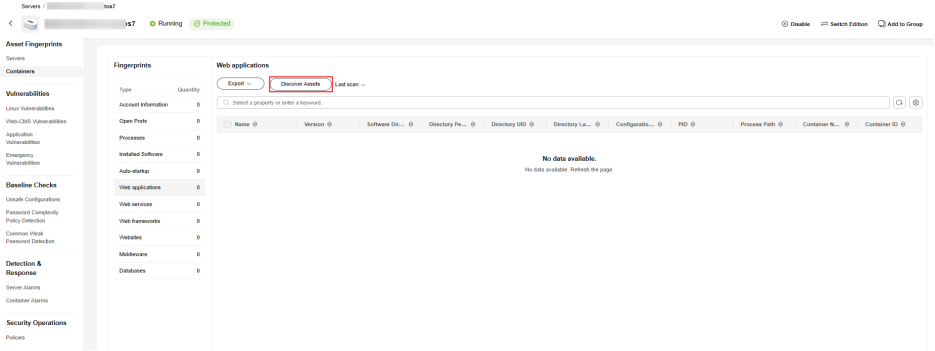
Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the name of the target server. On the server details page that is displayed, choose **Asset Fingerprints** > **Containers**.

Step 6 Click a fingerprint in the fingerprint list, and click **Discover Assets** on the upper area of the list on the right.

Currently, only **Web Applications**, **Web Services**, **Web Frameworks**, **Websites**, **Middleware**, and **Databases** support real-time manual collection and update. Information about other types is automatically collected and updated every day.

Figure 4-6 Collecting data now



Type	Quantity
Account Information	0
Open Ports	0
Processes	0
Installed Software	0
Auto-startup	0
Web applications	0
Web services	0
Web frameworks	0
Websites	0
Middleware	0
Databases	0

Name	Version	Software Dir...	Directory Pe...	Directory UID	Directory La...	Configuratio...	PID	Process Path	Container N...	Container ID

No data available.

No data available. Refresh the page.

Step 7 After the automatic execution is complete, the last scan time is updated and the latest container asset information is displayed.

----End

Manually Collecting the Latest Asset Fingerprints of All Containers

To view the latest data of accounts, open ports, processes, software, auto-started items, websites, web frameworks, middleware, web services, web applications, and databases in real time, you can manually collect their fingerprints.

Step 1 Log in to the management console.

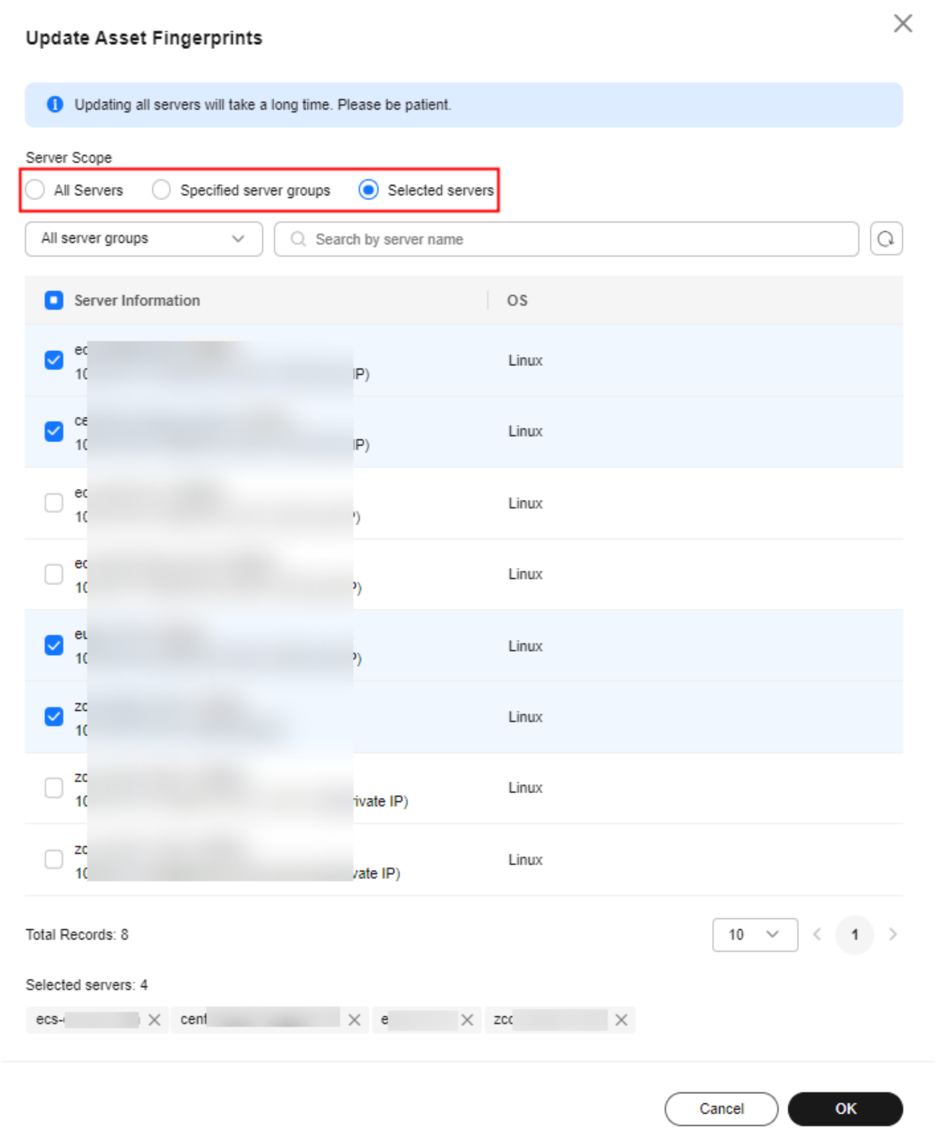
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Asset Management** > **Container Assets**.

Step 4 In the upper right corner of the page, click **Update Asset Fingerprints**.

Step 5 Select the server update scope and click **OK**.

Figure 4-7 Updating asset fingerprints



Update Asset Fingerprints

Updating all servers will take a long time. Please be patient.

Server Scope

○ All Servers ○ Specified server groups ● Selected servers

☑ Server Information	OS
☑ [redacted]	Linux
☑ [redacted]	Linux
□ [redacted]	Linux
□ [redacted]	Linux
☑ [redacted]	Linux
☑ [redacted]	Linux
□ [redacted]	Linux
□ [redacted]	Linux

Total Records: 8

Selected servers: 4

Step 6 After the **Updating Asset Fingerprints** status disappears from the button in the upper right corner of the page, you can view the latest asset fingerprints.

----End

Manually Collecting Cluster, Service, Workload, and Container Information

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management** > **Container Assets**.

Alternatively, you can choose **Installation & Configuration** > **Container Install & Config**, click the **Cluster** tab, and click **Synchronize the Latest Assets**.

Step 4 Click the **Cluster** tab and click **Synchronize Clusters** in the upper right corner.

Step 5 Wait for about 5 minutes, refresh the cluster page, and view the latest assets after synchronization.

----End

Follow-up Procedure

After the container fingerprints are collected, you can view the latest asset fingerprint data. For details, see **Viewing Container Assets**.

4.3.2 Viewing Container Assets

Scenarios

HSS can collect information about container assets, including clusters, nodes, containers, images, and container fingerprints. With the container asset function, you can centrally count container assets and detect unsafe assets in a timely manner.

This section describes how to view collected container asset information.

Constraints

- Only the HSS container edition supports the container fingerprint function.
- Only Linux is supported.

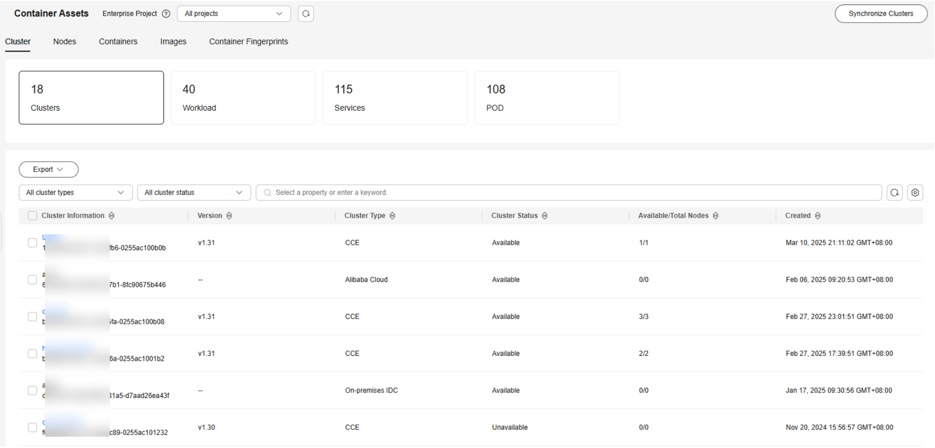
Viewing Cluster Information

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

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

Step 3 Choose **Asset Management** > **Container Assets**. Click the **Cluster** tab.

Figure 4-8 Clusters



18	40	115	108
Clusters	Workload	Services	POD

Cluster Information	Version	Cluster Type	Cluster Status	Available/Total Nodes	Created
[redacted]fb6-0255ac100b0b	v1.31	CCE	Available	1/1	Mar 10, 2025 21:11:02 GMT+08:00
[redacted]7b1-8fc90675b446	--	Alibaba Cloud	Available	0/0	Feb 06, 2025 09:20:53 GMT+08:00
[redacted]fa-0255ac100b08	v1.31	CCE	Available	3/3	Feb 27, 2025 23:01:51 GMT+08:00
[redacted]6a-0255ac1001b2	v1.31	CCE	Available	2/2	Feb 27, 2025 17:39:51 GMT+08:00
[redacted]1a5-d7aad26ea43f	--	On-premises IDC	Available	0/0	Jan 17, 2025 09:30:56 GMT+08:00
[redacted]c89-0255ac101232	v1.30	CCE	Unavailable	0/0	Nov 20, 2024 15:56:57 GMT+08:00

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View the cluster list, workload, service, and pod information.

----End

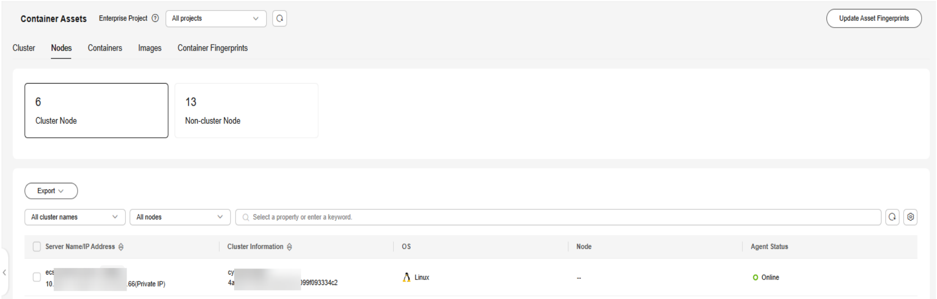
Viewing Node Information

Step 1 Log in to the management console.

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

Step 3 Choose **Asset Management** > **Container Assets**. Click the **Nodes** tab.

Figure 4-9 Nodes



6 Cluster Node

13 Non-cluster Node

Server Name/IP Address	Cluster Information	OS	Node	Agent Status
ecs[redacted] 10.66(Private IP)	cy[redacted] 4a99f093334c2	Linux	--	Online

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View information about cluster nodes and independent nodes.

----End

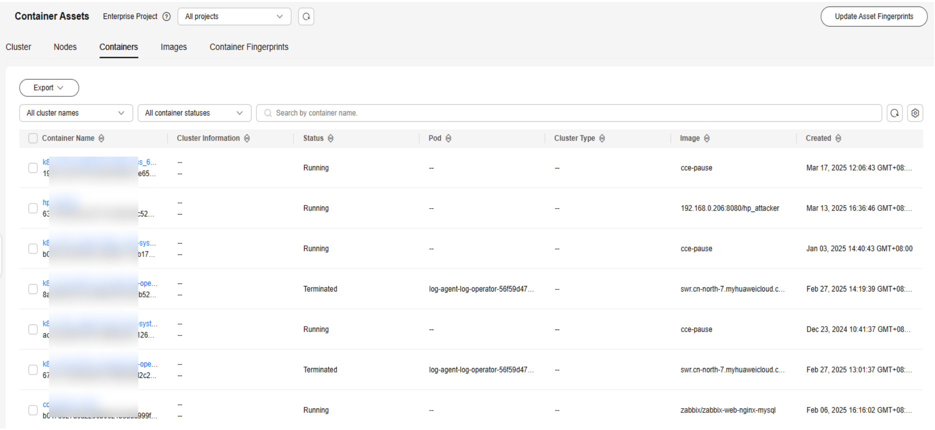
Viewing Container Information

Step 1 Log in to the management console.

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

Step 3 Choose **Asset Management** > **Container Assets**. Click the **Containers** tab.

Figure 4-10 Containers



Container Name	Cluster Information	Status	Pod	Cluster Type	Image	Created
k8[redacted]s_6... 19e65...	-- --	Running	--	--	cce-pause	Mar 17, 2025 12:06:43 GMT+08:...
hp[redacted] 63:52...	-- --	Running	--	--	192.168.0.206:8080/hp_attacker	Mar 13, 2025 16:36:46 GMT+08:...
k8[redacted]-sys... b0b17...	-- --	Running	--	--	cce-pause	Jan 03, 2025 14:40:43 GMT+08:00
k8[redacted]-ope... 8ab52...	-- --	Terminated	log-agent-log-operator-56f59d47...	--	swr.cn-north-7.myhuaweicloud.c...	Feb 27, 2025 14:19:39 GMT+08:...
k8[redacted]-syst... ac126...	-- --	Running	--	--	cce-pause	Dec 23, 2024 10:41:37 GMT+08...
k8[redacted]-ope... 67l2c2...	-- --	Terminated	log-agent-log-operator-56f59d47...	--	swr.cn-north-7.myhuaweicloud.c...	Feb 27, 2025 13:01:37 GMT+08:...
cc[redacted] b0999f...	-- --	Running	--	--	zabbix/zabbix-web-nginx-mysql	Feb 06, 2025 16:16:02 GMT+08:...

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View container information.

----End

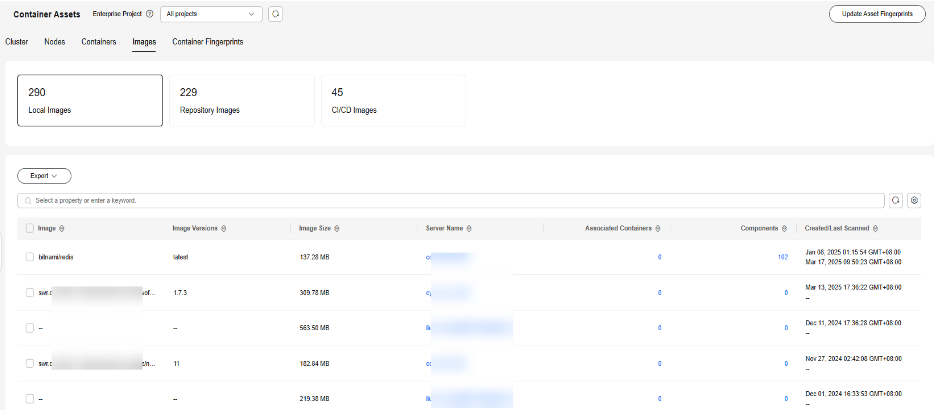
Viewing Image Information

Step 1 Log in to the management console.

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

Step 3 Choose **Asset Management** > **Container Assets**. Click the **Images** tab.

Figure 4-11 Images



Container Assets Enterprise Project All projects

Update Asset Fingerprints

Cluster Nodes Containers Images Container Fingerprints

290 Local Images

229 Repository Images

45 CI/CD Images

Export

Select a property or enter a keyword.

Image	Image Versions	Image Size	Server Name	Associated Containers	Components	Created/Last Scanned
bitnami/redis	latest	137.28 MB	cc[redacted]	0	102	Jan 08, 2025 01:15:54 GMT+08:00 Mar 17, 2025 09:50:23 GMT+08:00
swr.c[redacted]vof...	1.7.3	309.78 MB	cy[redacted]	0	0	Mar 13, 2025 17:36:22 GMT+08:00 --
--	--	563.50 MB	liu[redacted]	0	0	Dec 11, 2024 17:36:28 GMT+08:00 --
swr.c[redacted]z/n...	11	182.84 MB	cc[redacted]	0	0	Nov 27, 2024 02:42:08 GMT+08:00 --
--	--	219.38 MB	liu[redacted]	0	0	Dec 01, 2024 16:33:53 GMT+08:00 --

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View the CI/CD image, local image, and container image information.

----End

Viewing Container Fingerprint Information

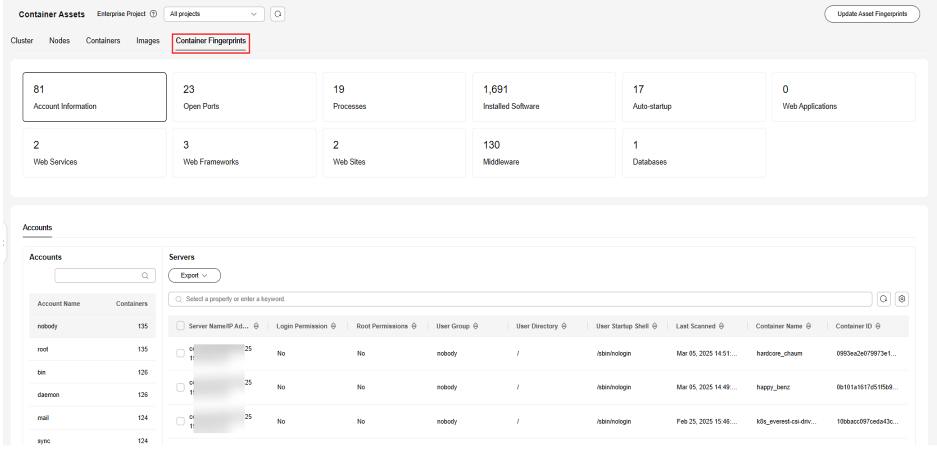
Step 1 Log in to the management console.

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

Step 3 Choose **Asset Management** > **Container Fingerprints**. Click the **Container Fingerprints** tab. View the fingerprint data of all containers.

To view the fingerprints of a single container, choose **Asset Management** > **Servers & Quota**, and click the server name where the container is deployed. On the node details page that is displayed, choose **Asset Fingerprints** > **Container Assets**.

Figure 4-12 Container fingerprints



81 Account Information	23 Open Ports	19 Processes	1,691 Installed Software	17 Auto-startup	0 Web Applications
2 Web Services	3 Web Frameworks	2 Web Sites	130 Middleware	1 Databases	

Account Name	Containers
nobody	135
root	135
bin	126
daemon	126
mail	124
sync	124

Server Name/IP Ad...	Login Permission	Root Permissions	User Group	User Directory	User Startup Shell	Last Scanned	Container Name	Container ID
[redacted]	No	No	nobody	/	/sbin/nologin	Mar 05, 2025 14:51:...	hardcore_chaum	0993ea2e079973e1...
[redacted]	No	No	nobody	/	/sbin/nologin	Mar 05, 2025 14:49:...	happy_benz	0b101a1617d51f5b9...
[redacted]	No	No	nobody	/	/sbin/nologin	Feb 25, 2025 15:46:...	k8s_everest-csi-driv...	10bbacc097ceda43c...

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click a fingerprint type in the list to view the asset information.

Step 6 (Optional) Remove risky assets.

If you find unsafe assets after counting, remove them in a timely manner.

If you receive port alarms, you can set **Dangerous Port** to **Yes** in the search box of the **Open Ports** area to filter dangerous ports. You are advised to handle unsafe ports as follows:

- If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. If they are not, disable them. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.
- If a detected high-risk port is actually a normal port used for services, you can ignore it. Ignored alarms will neither be recorded as unsafe items and nor trigger alarms.

High-risk port list describes the common dangerous ports.

----End

4.4 Server Management

4.4.1 Viewing Server Protection Status

You are advised to periodically check the server protection status and handle security risks in a timely manner to prevent asset loss.

The server list on the **Servers & Quota** page displays the protection status of only the following servers:

- Huawei Cloud servers purchased in the selected region
- Non-Huawei Cloud servers that have been added to the selected region

Viewing Server Protection Status

Step 1 Log in to the management console.

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

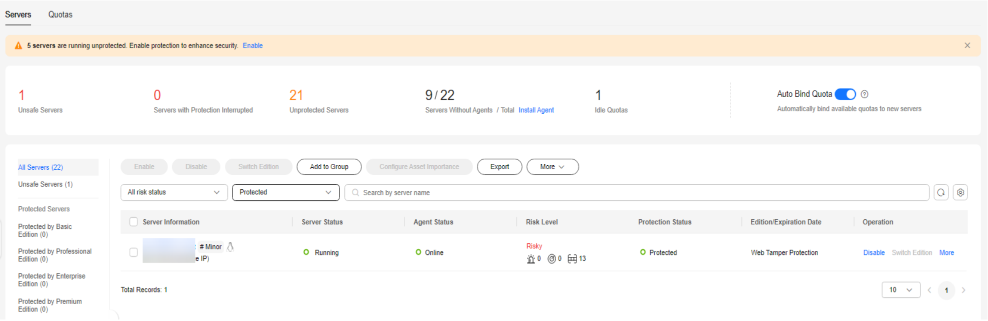
Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the server list, view the protection status of servers. For details, see **Server protection status**.

You can also view the server name, ID, IP address, OS, status, and enterprise project on the **Servers** tab. To select the items to be displayed in the server protection list, click ⚙ in the upper right corner of the list.

Figure 4-13 Server protection status


Servers
Quotas
5 servers are running unprotected. Enable protection to enhance security. Enable
1
Unsafe Servers
0
Servers with Protection Interrupted
21
Unprotected Servers
9 / 22
Servers Without Agents / Total Install Agent
1
Idle Quotas
Auto Bind Quota
Automatically bind available quotas to new servers
All Servers (22)
Unsafe Servers (1)
Protected Servers
Protected by Basic Edition (0)
Protected by Professional Edition (0)
Protected by Enterprise Edition (0)
Protected by Premium Edition (0)
Enable
Disable
Switch Edition
Add to Group
Configure Asset Importance
Export
More
All risk status
Protected
Search by server name

Server Information	Server Status	Agent Status	Risk Level	Protection Status	Edition/Expiration Date	Operation
[redacted] # Minor e IP)	Running	Online	Risky 0 0 13	Protected	Web Tamper Protection	Disable Switch Edition More

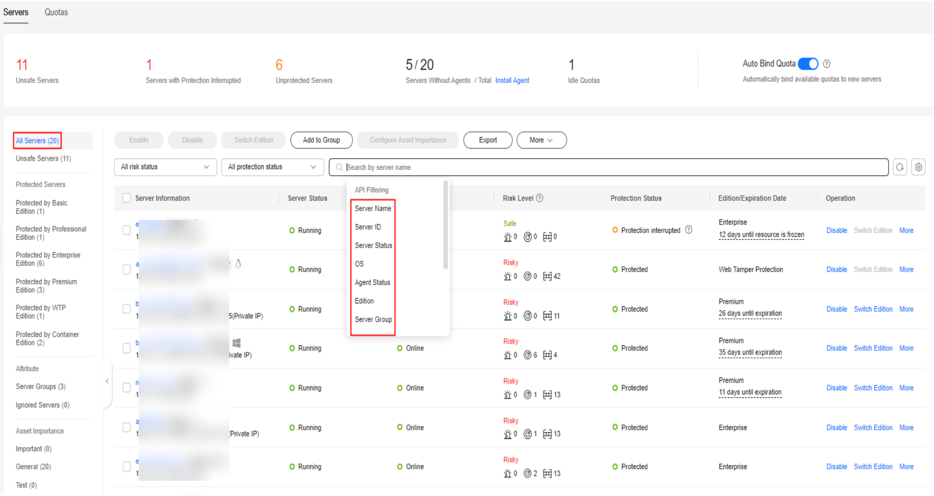
Total Records: 1

10 < 1 >

- **Searching for a server**

  To check the protection status of a server, enter a server name, server ID, or IP address in the search box above the server protection list.

  Figure 4-14 Searching for a protected server



Server Information	Server Status		Risk Level	Protection Status	Edition/Expiration Date	Operation
[redacted]	Running		Safe 0 0 0	Protection interrupted	Enterprise 12 days until resource is frozen	Disable Switch Edition More
[redacted]	Running		Risky 0 0 42	Protected	Web Tamper Protection	Disable Switch Edition More
[redacted] 5(Private IP)	Running		Risky 0 0 11	Protected	Premium 26 days until expiration	Disable Switch Edition More
[redacted] ivate IP)	Running	Online	Risky 0 6 4	Protected	Premium 35 days until expiration	Disable Switch Edition More
[redacted]	Running	Online	Risky 0 1 13	Protected	Premium 11 days until expiration	Disable Switch Edition More
[redacted] Private IP)	Running	Online	Risky 0 1 13	Protected	Enterprise	Disable Switch Edition More
[redacted]	Running	Online	Risky 0 2 13	Protected	Enterprise	Disable Switch Edition More

- **Viewing servers of a certain type**

  On the left of the server protection list, select a server protection edition or an asset importance category to view the protection status of each type of servers.

- **Viewing server details**

  Hover your cursor over a server name to view details about the server OS, system version, and kernel version.

- **Viewing server protection information**

  The **Protection Status** column indicates whether a server is protected. The protection status of a server is determined by **Agent Status** and **Server Status**. You can view the server risk detection status in the **Risk Level** column. For details about the preceding parameters, see **Table 4-7**.

Table 4-7 Protection description

Parameter	Description
Server Status	HSS can only protect running servers. If the server is in the **Stopped** or other state, you cannot perform security checks or fix risks on the server.
Agent Status	– **Not installed**: The agent has not been installed or successfully started. Click **Install Agent** and install the agent as prompted. For details, see **Installing an Agent**. – **Online**: The agent has been installed and running properly. – **Offline**: The agent has been installed, but the agent is disconnected from the HSS remote protection center. In this case, HSS cannot provide protection. For more information, see **How Do I Fix an Abnormal Agent?** NOTE For an IDC server, its information will be automatically deleted from the server management page after its agent goes offline for 30 days. – **Installation failed**: An error or problem occurred, leading to an installation failure. Click ? next to the installation failure status to view the cause. Rectify the fault by referring to **What Should I Do If Agent Installation Failed?** – **Installing**: The agent is being installed.
Protection Status	– **Enabled**: The server is fully protected by HSS. – **Unprotected**: HSS is disabled for the server. After the agent is installed, click **Enable** in the **Operation** column to enable protection. – **Protection interrupted**: The server is shut down, the agent is offline, or the agent is uninstalled. You can hover the cursor on ? next to **Protection interrupted** to view the cause.

Parameter	Description
Risk Level	Risk status of a server. (Data is updated every 24 hours.) – **Risky**: The server has risks. Hover your cursor over a risk icon to view risk distribution details. Click a risk quantity to go to the risk details page. – **Safe**: No risks are found. – **Pending risk detection**: HSS is not enabled for the server.

----End

Viewing the WTP Status

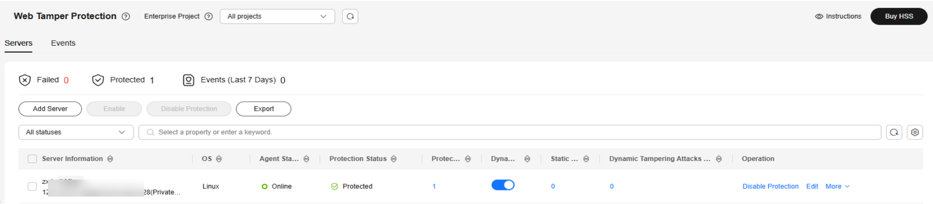
Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Server Protection** > **Web Tamper Protection**. The **Servers** tab page is displayed.

Step 3 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 4 Check the server protection status.

Figure 4-15 Servers protected by WTP



☐ Server Information	OS	Agent Sta...	Protection Status	Protec...	Dyna...	Static ...	Dynamic Tampering Attacks ...	Operation
☐ zx[redacted] 12[redacted]28(Private...	Linux	Online	Protected	1	●	0	0	Disable Protection Edit More

Table 4-8 Statuses

Parameter	Description
Agent Status	● **Not installed**: The agent has not been installed or successfully started. Click **Install Agent** and install the agent as prompted. For details, see **Installing an Agent**. ● **Online**: The agent has been installed and running properly. ● **Offline**: The agent has been installed, but the agent is disconnected from the HSS remote protection center. In this case, HSS cannot provide protection. For more information, see **How Do I Fix an Abnormal Agent?** NOTE For an IDC server, its information will be automatically deleted from the server management page after its agent goes offline for 30 days. ● **Installation failed**: An error or problem occurred, leading to an installation failure. Click ? next to the installation failure status to view the cause. Rectify the fault by referring to **What Should I Do If Agent Installation Failed?** ● **Installing**: The agent is being installed.
Protection Status	WTP status. ● **Enabling**: Static WTP is being enabled. ● **Protected**: Static WTP protection is enabled for all protected directories. ● **Partially protected**: Static WTP protection is enabled for some protected directories and disabled for others. ● **Protection failed**: Static WTP protection fails to be enabled for at least one protected directory. ● **Protection interrupted**: The server is shut down, the agent is offline, or the agent is uninstalled. You can hover the cursor on ? next to **Protection interrupted** to view the cause. ● **Protection suspended**: Static WTP protection is suspended for all protected directories. ● **Unprotected**: Static WTP protection is not enabled for a server.
Protected Directories	Number of directories added for static WTP protection. You can click the number to go to the protected directory details page.

Parameter	Description
Dynamic WTP	Status of dynamic WTP, which can be: - ⬤: Dynamic WTP is enabled. - ○: Dynamic WTP is disabled. (After enabling dynamic WTP, restart Tomcat to make this setting take effect.)
Static Tampering Attacks	Number of times that static web page files are attacked and tampered with.
Dynamic Tampering Attacks	Number of web application vulnerability exploits and injection attacks.

----End

FAQ

Protection Interrupted

4.4.2 Viewing the Assets and Risks of a Server

Scenario

HSS can display asset fingerprints, vulnerability management, baseline inspection, detection and response, and policy management in the function or server dimension to facilitate risk handling.

- Function dimension: The assets or risks of all servers or containers are displayed on a single page for you to check and handle.
- Server dimension: The assets or risks of a single server or container node is displayed, so that you can handle the risks of an important asset first.

This section describes how to view assets and risks by server.

Viewing the Assets and Risks of a Server

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

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

Step 3 In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**.

Step 4 Click the name of a server to go to the server details page.

Step 5 On the server details page, check **Asset Fingerprints**, **Vulnerability Management**, **Baseline Checks**, **Detection & Response**, and **Policy Management**.

----End

Asset Fingerprints

The asset fingerprint page displays server and container fingerprints. For more information, see **Server Fingerprints** and **Container Assets**.

To view asset fingerprints, perform the following steps:

1. Choose a fingerprint page as needed.

   To check server fingerprints, choose the **Server Fingerprints** page. To check container fingerprints, choose the **Container Fingerprints** page.

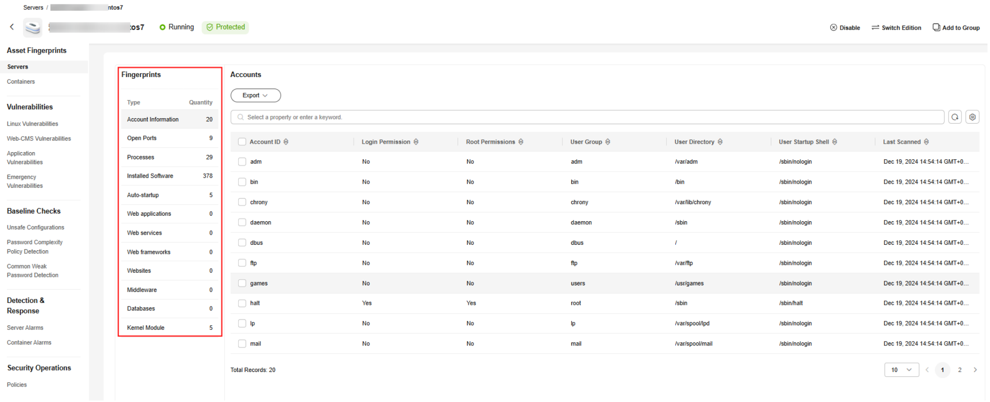
2. In the fingerprint list, select a fingerprint type to view its details.

   Server and container fingerprints include:

   – Server fingerprints: accounts, open ports, processes, software, auto-started items, web applications, web services, web frameworks, websites, middleware, kernel modules, and databases

   – Container fingerprints: accounts, open ports, processes, software, auto-started items, web applications, web services, web frameworks, websites, middleware, and databases

Figure 4-16 Asset fingerprints



Servers / [redacted]ntos7

[redacted]:os7 Running Protected

Fingerprints

Type	Quantity
Account Information	20
Open Ports	9
Processes	29
Installed Software	378
Auto-startup	5
Web applications	0
Web services	0
Web frameworks	0
Websites	0
Middleware	0
Databases	0
Kernel Module	5

Accounts

Account ID	Login Permission	Root Permissions	User Group	User Directory	User Startup Shell	Last Scanned
adm	No	No	adm	/var/adm	/sbin/nologin	Dec 19, 2024 14:54:14 GMT+0...
bin	No	No	bin	/bin	/sbin/nologin	Dec 19, 2024 14:54:14 GMT+0...
chrony	No	No	chrony	/var/lib/chrony	/sbin/nologin	Dec 19, 2024 14:54:14 GMT+0...
daemon	No	No	daemon	/sbin	/sbin/nologin	Dec 19, 2024 14:54:14 GMT+0...
dbus	No	No	dbus	/	/sbin/nologin	Dec 19, 2024 14:54:14 GMT+0...
ftp	No	No	ftp	/var/ftp	/sbin/nologin	Dec 19, 2024 14:54:14 GMT+0...
games	No	No	users	/usr/games	/sbin/nologin	Dec 19, 2024 14:54:14 GMT+0...
halt	Yes	Yes	root	/sbin	/sbin/halt	Dec 19, 2024 14:54:14 GMT+0...
lp	No	No	lp	/var/spool/lpd	/sbin/nologin	Dec 19, 2024 14:54:14 GMT+0...
mail	No	No	mail	/var/spool/mail	/sbin/nologin	Dec 19, 2024 14:54:14 GMT+0...

Total Records: 20

3. (Optional) If you find unsafe assets after counting, remove them in a timely manner.

   If you receive a dangerous port alarm, in the search box above the list in the **Open Ports** area, set **Dangerous Port** to **Yes** to filter dangerous ports. You are advised to handle dangerous ports as follows:

   – If HSS detects open dangerous ports or unused ports, check whether they are really used by your services. If they are not, disable them. For dangerous ports, you are advised to further check their program files, and delete or isolate their source files if necessary.

   – If a detected dangerous port is actually a normal port used for services, you can ignore it. Ignored alarms will neither be recorded as unsafe items and nor trigger alarms.

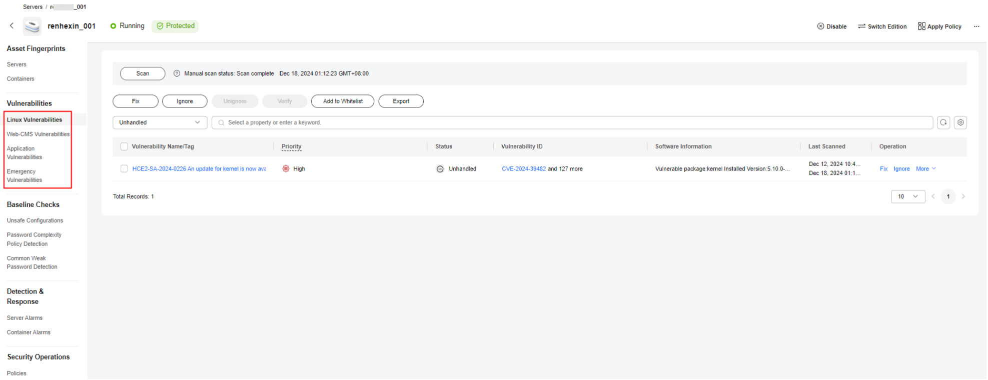
Vulnerability Management

The vulnerability management page displays Linux vulnerabilities, Windows vulnerabilities, Web-CMS vulnerabilities, application vulnerabilities, and emergency vulnerabilities. For more information, see **Vulnerability Management Overview**.

To view vulnerability information, perform the following steps:

1. Select a vulnerability type to view corresponding vulnerabilities.

Figure 4-17 Vulnerability management



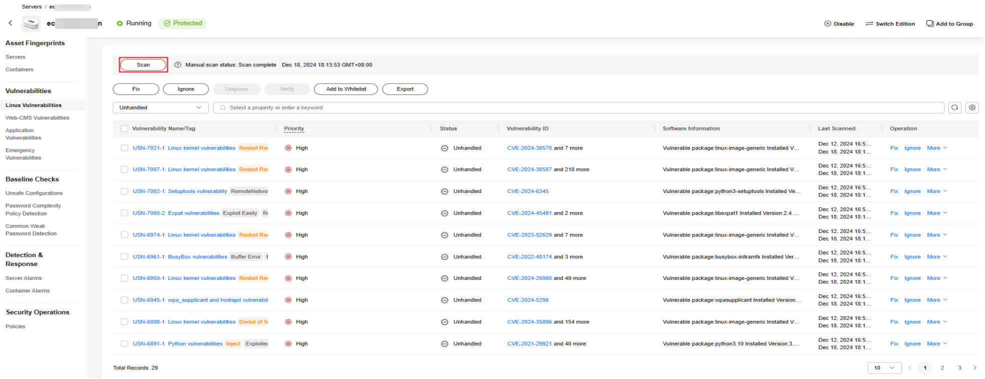
Manual scan status: Scan complete Dec 18, 2024 01:12:23 GMT+08:00

Vulnerability Name/Tag	Priority	Status	Vulnerability ID	Software Information	Last Scanned	Operation
HCE2-SA-2024-0226 An update for kernel is now ava	High	Unhandled	CVE-2024-39482 and 127 more	Vulnerable package:kernel Installed Version:5.10.0-...	Dec 12, 2024 10:4... Dec 18, 2024 01:1...	Fix Ignore More

Total Records: 1

2. In the upper left corner of the page, click **Scan** to scan for vulnerabilities immediately.

Figure 4-18 Manual scan



Manual scan status: Scan complete Dec 18, 2024 18:13:53 GMT+08:00

Vulnerability Name/Tag	Priority	Status	Vulnerability ID	Software Information	Last Scanned	Operation
USN-7021-1: Linux kernel vulnerabilities Restart Rec	High	Unhandled	CVE-2024-38570 and 7 more	Vulnerable package:linux-image-generic Installed V...	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More
USN-7007-1: Linux kernel vulnerabilities Restart Rec	High	Unhandled	CVE-2024-38587 and 218 more	Vulnerable package:linux-image-generic Installed V...	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More
USN-7002-1: Setuptools vulnerability RemoteNetwo	High	Unhandled	CVE-2024-6345	Vulnerable package:python3-setuptools Installed Ve...	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More
USN-7000-2: Expat vulnerabilities Exploit Easily R	High	Unhandled	CVE-2024-45491 and 2 more	Vulnerable package:libexpat1 Installed Version:2.4....	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More
USN-6974-1: Linux kernel vulnerabilities Restart Rec	High	Unhandled	CVE-2023-52629 and 7 more	Vulnerable package:linux-image-generic Installed V...	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More
USN-6961-1: BusyBox vulnerabilities Buffer Error E	High	Unhandled	CVE-2022-48174 and 3 more	Vulnerable package:busybox-initramfs Installed Ver...	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More
USN-6950-1: Linux kernel vulnerabilities Restart Rec	High	Unhandled	CVE-2024-26980 and 49 more	Vulnerable package:linux-image-generic Installed V...	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More
USN-6945-1: wpa_supplicant and hostapd vulnerabili	High	Unhandled	CVE-2024-5290	Vulnerable package:wpasupplicant Installed Version...	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More
USN-6898-1: Linux kernel vulnerabilities Denial of S	High	Unhandled	CVE-2024-35896 and 154 more	Vulnerable package:linux-image-generic Installed V...	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More
USN-6891-1: Python vulnerabilities Inject Exploitec	High	Unhandled	CVE-2021-29921 and 40 more	Vulnerable package:python3.10 Installed Version:3....	Dec 12, 2024 16:5... Dec 18, 2024 18:1...	Fix Ignore More

Total Records: 29

3. For details about how to handle vulnerabilities (add to whitelist, fix, or ignore), see **Handling Vulnerabilities**.

   For details about how to fix a vulnerability, see "Automatically Fixing Vulnerabilities (Vulnerability View)" and "Manually Fixing Vulnerabilities" in "Handling Vulnerabilities".

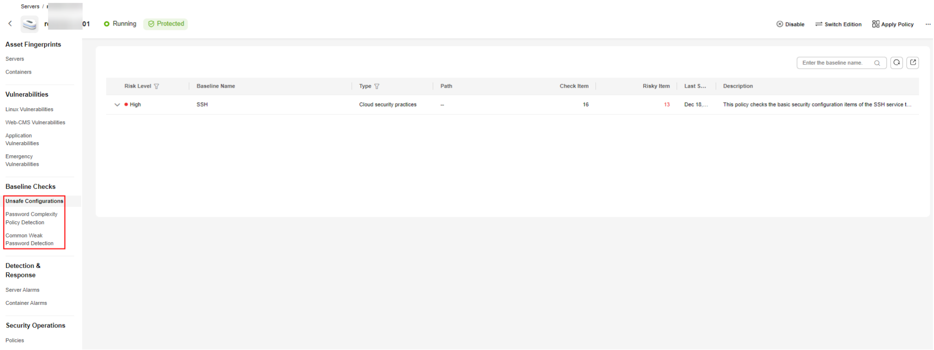
Baseline Checks

Baseline checks show the results of unsafe baseline settings, password complexity policy risks, and common weak password risks. For more information, see **Baseline Check Overview**.

To view baseline check information, perform the following steps:

1. Select a check type.

Figure 4-19 Baseline checks



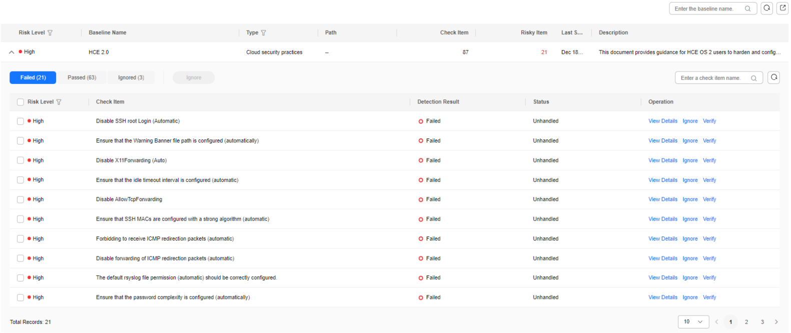
Risk Level	Baseline Name	Type	Path	Check Item	Risky Item	Last S...	Description
● High	SSH	Cloud security practices	--	16	13	Dec 18,...	This policy checks the basic security configuration items of the SSH service t...

2. View check results.

   – **Unsafe Settings**

   i. Click ⌄ in the **Risk Level** column to expand baseline details.

Figure 4-20 Unsafe configurations



Risk Level	Baseline Name	Type	Path	Check Item	Risky Item	Last S...	Description
● High	HCE 2.0	Cloud security practices	--	87	21	Dec 18...	This document provides guidance for HCE OS 2 users to harden and config...

Risk Level	Check Item	Detection Result	Status	Operation
● High	Disable SSH root Login (Automatic)	Failed	Unhandled	View Details Ignore Verify
● High	Ensure that the Warning Banner file path is configured (automatically)	Failed	Unhandled	View Details Ignore Verify
● High	Disable X11Forwarding (Auto)	Failed	Unhandled	View Details Ignore Verify
● High	Ensure that the idle timeout interval is configured (automatic)	Failed	Unhandled	View Details Ignore Verify
● High	Disable AllowTcpForwarding	Failed	Unhandled	View Details Ignore Verify
● High	Ensure that SSH MACs are configured with a strong algorithm (automatic)	Failed	Unhandled	View Details Ignore Verify
● High	Forbidding to receive ICMP redirection packets (automatic)	Failed	Unhandled	View Details Ignore Verify
● High	Disable forwarding of ICMP redirection packets (automatic)	Failed	Unhandled	View Details Ignore Verify
● High	The default rsyslog file permission (automatic) should be correctly configured.	Failed	Unhandled	View Details Ignore Verify
● High	Ensure that the password complexity is configured (automatically)	Failed	Unhandled	View Details Ignore Verify

Total Records: 21

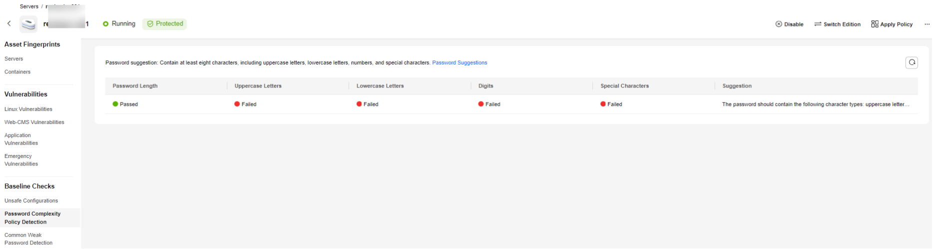
   ii. On the **Failed** tab page, view the baseline items that failed the check.

   iii. In the row of a baseline item, click **View Details** in the **Operation** column to view the check item description, audit description, and suggestions.

   You can fix the baseline items that failed to pass the check based on the suggestions. For details, see **Viewing and Handling Baseline Configuration Risks**.

   – **Password Complexity Policy Risks**

Figure 4-21 Password complexity policy check



Password suggestion: Contain at least eight characters, including uppercase letters, lowercase letters, numbers, and special characters. Password Suggestions

Password Length	Uppercase Letters	Lowercase Letters	Digits	Special Characters	Suggestion
● Passed	● Failed	● Failed	● Failed	● Failed	The password should contain the following character types: uppercase letter...

   If the password complexity policy of a server does not meet related standards, log in to the server and modify the password complexity policy.

- To monitor the password complexity policy on a Linux server, install the Pluggable Authentication Modules (PAM) on the server. For details, see **How Do I Install a PAM in a Linux OS?**
- For details about how to modify the password complexity policy on a Linux server, see **How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS?**
- For details about how to modify the password complexity policy on a Windows server, see **How Do I Set a Secure Password Complexity Policy in a Windows OS?**

– Common Weak Password Risks

To view the latest weak password detection data, click **Scan** in the upper left corner of the page to scan for weak passwords on the server.

You are advised to log in to the server and change the weak passwords as soon as possible.

Detection & Response

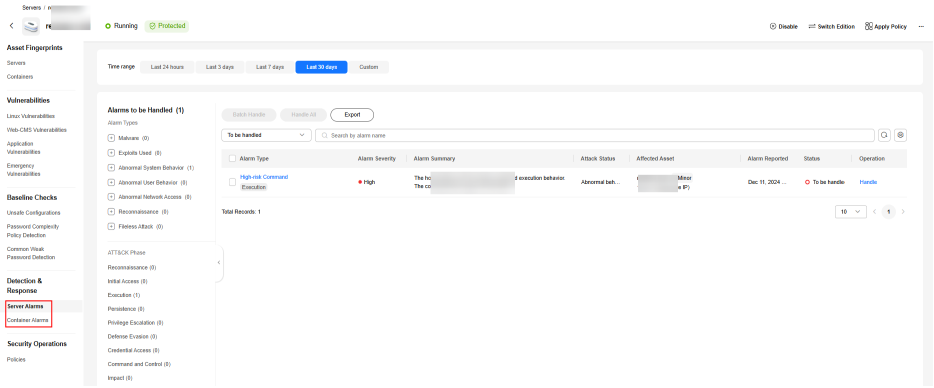
The detection and response page displays intrusion detection alarms, including server security alarms and container security alarms. For more information, see **Server Alarms** and **Container Alarm Events**.

To view intrusion detection information, perform the following steps:

Step 1 Select an alarm type and view the alarm event list.

To view server alarms, choose **Server Alarms**. To view container alarms, choose **Container Alarms**.

Figure 4-22 Server alarms



Alarm Type	Alarm Severity	Alarm Summary	Attack Status	Affected Asset	Alarm Reported	Status	Operation
High-risk Command Execution	High	The ho[redacted]d execution behavior. The co	Abnormal beh...	[redacted]Minor e IP)	Dec 11, 2024 ...	To be handle	Handle

Step 2 Click an alarm name to view the alarm details, forensics, and similar alarms.

Step 3 In the **Operation** column of an alarm, click **Handle** to handle the alarm.

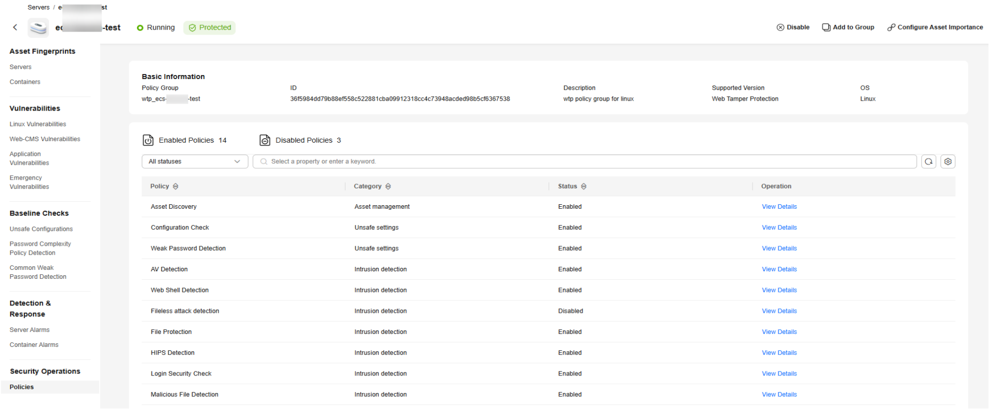
For details, see **Handling Server Alarms** and **Handling Container Alarms**.

----End

Policy Management

To view the application of all the policies in the policy group associated with the current server or container node, choose **Security Operations** > **Policies**. For more information, see **Policy Management Overview**.

Figure 4-23 Policy management



Basic Information

Policy Group	ID	Description	Supported Version	OS
wtp_ecs-[redacted]-test	36f5984dd79b88ef558c522881cba09912318cc4c73948acded98b5cf6367538	wtp policy group for linux	Web Tamper Protection	Linux

Policy	Category	Status	Operation
Asset Discovery	Asset management	Enabled	View Details
Configuration Check	Unsafe settings	Enabled	View Details
Weak Password Detection	Unsafe settings	Enabled	View Details
AV Detection	Intrusion detection	Enabled	View Details
Web Shell Detection	Intrusion detection	Enabled	View Details
Fileless attack detection	Intrusion detection	Disabled	View Details
File Protection	Intrusion detection	Enabled	View Details
HIPS Detection	Intrusion detection	Enabled	View Details
Login Security Check	Intrusion detection	Enabled	View Details
Malicious File Detection	Intrusion detection	Enabled	View Details

- **Basic Information**: In the **Basic Information** area, you can view basic information about the policy group.
- **Status**: In the row of a policy, view its status in the **Status** column.
  - **Disabled**: The policy is disabled.
  - **Enabled**: The policy is enabled.
  - **Enabling**: The policy is being enabled. This state lasts for 2 to 3 minutes.
  - **Enabling failed**: The protection capabilities of the agent are degraded due to some exceptions. As a result, some policies failed to be enabled. For details about the cause and solution of agent protection degradation, see **Protection Degradation**.

  To enable or disable a policy, perform the following steps:

  a. On the home page of the HSS console, choose **Security Operations** > **Policies**.

  b. Click the name of the target policy group. The policy list page is displayed.

  c. In the row containing the target self-protection policy, click **Enable** or **Disable** in the **Operation** column.
- **Policy Details**: In the row containing the target policy, click **View Details** in the **Operation** column to view the policy details.

4.4.3 Exporting the Server List

This section describes how to export the server protection list to your local PC.

Exporting the Server List to the Local PC

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

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

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The **Servers** tab is displayed.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the upper right corner of the server list, click **Export** to export the server list details.

You can also select specified servers in the server list and click **Export**. The details of up to 1000 servers can be exported at a time.

----End

4.4.4 Switching the HSS Quota Edition

You can switch the quota edition of a server to the basic, professional, enterprise, premium, or container edition as needed.

Precautions

You can switch to the basic, professional, enterprise or premium edition.

To use the WTP or container edition, purchase a quota of that edition and then enable it. For details, see **Purchasing an HSS Quota**.

Prerequisites

- Choose **Asset Management** > **Servers & Quota**. On the **Servers** tab, the protection status of a server is **Protected**.
- Before switching to a quota in yearly/monthly billing mode, ensure the quota has been purchased and is available. For details, see **Purchasing an HSS Quota**.
- Before switching to a lower edition, check the server, handle known risks, and record operation information to prevent O&M errors and attacks.

Switching the HSS Quota Edition

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

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

Step 3 In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**. The **Servers** tab is displayed.

NOTE

The server list displays the protection status of only the following servers:

- Huawei Cloud servers purchased in the selected region
- Non-Huawei Cloud servers that have been added to the selected region

Step 4 You can switch the quota editions for one or multiple servers.

- Switching the quota edition for a single server
  a. In the **Operation** column of a server, click **Switch Edition**.
  b. In the **Configure Protection** area, select a billing mode, an edition, and a quota. For more information, see **Table 4-9**.

Table 4-9 Parameters for switching editions

Parameter	Description
Billing Mode	Billing mode of a quota. ■ Yearly/Monthly ■ Pay-per-use
Edition	Select a quota edition. ■ Basic edition: It protects test servers or individual users' servers. **It can protect any number of servers, but only part of the security scan capabilities are available**. **This edition does not provide protection capabilities, nor does it provide support for the DJCP Multi-level Protection Scheme (MLPS) certification**. The basic edition is free of charge for 30 days if it was enabled for the first time. ■ Professional edition: This edition is higher than the basic edition but lower than the enterprise edition. Its features include file directory change detection, abnormal shell detection, and policy management. ■ Enterprise edition: Main features include asset fingerprint management, vulnerability management, malicious program detection, web shell detection, and abnormal process behavior detection. ■ Premium edition: Main features include application protection, ransomware prevention, high-risk command detection, privilege escalation detection, and abnormal shell detection. ■ Container edition: It protects containers throughout their lifecycle, including building, deployment, and running. For details about the differences between the editions, see **Features**.

Parameter	Description
Select Quota	If you select **Yearly/Monthly**, you need to select a protection quota for the server. ▪ **Select a quota randomly**: A random quota is allocated to the server. ▪ Quota ID: The specified quota is bound to the server. When you switch the edition for multiple servers at a time, the quota you select can only be bound to one of them. The rest of the servers will be randomly bound to the quotas of the target edition. **NOTE** If the system displays a message indicating that there are no available quotas, you need to purchase quotas first.
Tags (optional)	If you select the pay-per-use billing mode, you can add tags to pay-per-use quotas. Tags are used to identify cloud resources. When you have many cloud resources of the same type, you can use tags to classify cloud resources by dimension (for example, by usage, owner, or environment).

c. Read the *Host Security Service Disclaimer* and select **I have read and agree to the Host Security Service Disclaimer**.

- Switching the quota editions for multiple servers

  a. Select multiple servers and click **Enable** above the server list.

  b. In the dialog box that is displayed, confirm the server information and select a billing mode, an edition, and a quota. For more information, see **Table 4-9**.

  c. Read the *Host Security Service Disclaimer* and select **I have read and agree to the Host Security Service Disclaimer**.

Step 5 Click **OK**.

The edition information in the **Edition** column will be updated. If the edition information in the **Edition** column is updated, the HSS edition switch succeeded.

----End

Follow-up Procedure

- After the edition is switched, you can allocate the idle edition quota to other servers.
- After switching to a lower edition, clear important data on the server, stop important applications on the server, and disconnect the server from the external network to avoid unnecessary loss caused by attacks.
- After switching to a higher edition, perform a security detection on the server, handle security risks on the server, and configure necessary functions in a timely manner.

4.4.5 Deploying a Protection Policy

You can quickly configure and start server scans by using policy groups. Simply create a group, add policies to it, and apply this group to servers. The agents deployed on your servers will scan everything specified in the policies.

Precautions

When the professional, enterprise, premium, WTP, or container edition is enabled, the protection policy group of the corresponding edition is deployed by default and applies to servers. You do not need to manually deploy policies. For premium and container editions, you can copy a policy group and customize it as required. To flexibly manage server protection policies, you can replace the default policy group with a custom policy group.

Creating a Policy Group

Step 1 Log in to the management console.

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

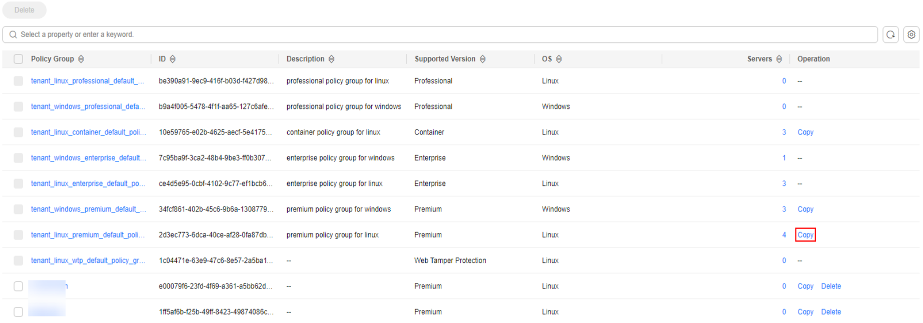
Step 3 In the navigation tree on the left, choose **Security Operations** > **Policies**

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Copy a policy group.

- Select the **tenant_linux_premium_default_policy_group** policy group. Locate the row that this policy group resides, click **Copy** in the **Operation** column.

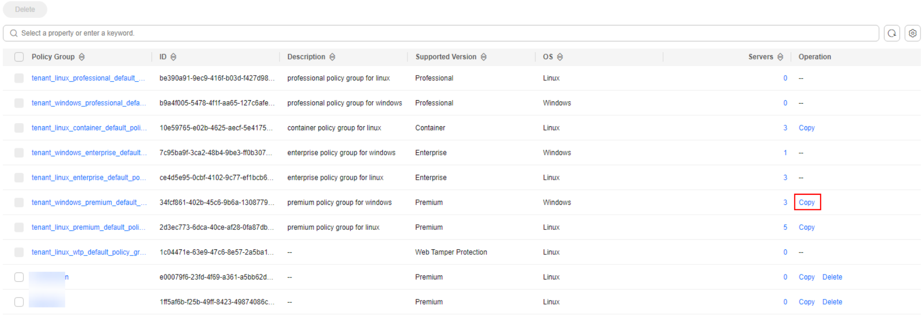
Figure 4-24 Copying a Linux policy group



Policy Group	ID	Description	Supported Version	OS	Servers	Operation
tenant_linux_professional_default_...	be390a91-9ec9-416f-b03d-f427d98...	professional policy group for linux	Professional	Linux	0	--
tenant_windows_professional_defa...	b9a4f005-5478-4f1f-aa65-127c6afe...	professional policy group for windows	Professional	Windows	0	--
tenant_linux_container_default_poli...	10e59765-e02b-4625-aecf-5e4175...	container policy group for linux	Container	Linux	3	Copy
tenant_windows_enterprise_default...	7c95ba9f-3ca2-48b4-9be3-ff0b307...	enterprise policy group for windows	Enterprise	Windows	1	--
tenant_linux_enterprise_default_po...	ce4d5e95-0cbf-4102-9c77-ef1bcb6...	enterprise policy group for linux	Enterprise	Linux	3	--
tenant_windows_premium_default_...	34fcf861-402b-45c6-9b6a-1308779...	premium policy group for windows	Premium	Windows	3	Copy
tenant_linux_premium_default_poli...	2d3ec773-6dca-40ce-af28-0fa87db...	premium policy group for linux	Premium	Linux	4	Copy
tenant_linux_wtp_default_policy_gr...	1c04471e-63e9-47c6-8e57-2a5ba1...	--	Web Tamper Protection	Linux	0	--
[redacted]	e00079f6-23fd-4f69-a361-a5bb62d...	--	Premium	Linux	0	Copy Delete
[redacted]	1ff5af6b-f25b-49ff-8423-49874086c...	--	Premium	Linux	0	Copy Delete

- Select the **tenant_windows_premium_default_policy_group** policy group. Click **Copy** in the **Operation** column.

Figure 4-25 Copying a Windows policy group



Policy Group	ID	Description	Supported Version	OS	Servers	Operation
tenant_linux_professional_default_...	be390a91-9ec9-416f-b03d-f427d98...	professional policy group for linux	Professional	Linux	0	--
tenant_windows_professional_defa...	b9a4f005-5478-4f1f-aa65-127c6afe...	professional policy group for windows	Professional	Windows	0	--
tenant_linux_container_default_poli...	10e59765-e02b-4625-aecf-5e4175...	container policy group for linux	Container	Linux	3	Copy
tenant_windows_enterprise_default...	7c95ba9f-3ca2-48b4-9be3-ff0b307...	enterprise policy group for windows	Enterprise	Windows	1	--
tenant_linux_enterprise_default_po...	ce4d5e95-0cbf-4102-9c77-ef1bcb6...	enterprise policy group for linux	Enterprise	Linux	3	--
tenant_windows_premium_default_...	34fcf861-402b-45c6-9b6a-1308779...	premium policy group for windows	Premium	Windows	3	Copy
tenant_linux_premium_default_poli...	2d3ec773-6dca-40ce-af28-0fa87db...	premium policy group for linux	Premium	Linux	5	Copy
tenant_linux_wtp_default_policy_gr...	1c04471e-63e9-47c6-8e57-2a5ba1...	--	Web Tamper Protection	Linux	0	--
[redacted]n	e00079f6-23fd-4f69-a361-a5bb62d...	--	Premium	Linux	0	Copy Delete
[redacted]	1ff5af6b-f25b-49ff-8423-49874086c...	--	Premium	Linux	0	Copy Delete

Step 6 In the dialog box displayed, enter a policy group name and description, and click **OK**.

- The name of a policy group must be unique, or the group will fail to be created.
- The policy group name and its description can contain only letters, digits, underscores (_), hyphens (-), and spaces, and cannot start or end with a space.

Step 7 Click **OK**.

Step 8 Click the name of the policy group you just created. The policies in the group will be displayed.

Step 9 Click a policy name and modify its settings as required. For details, see **Configuring Policies**.

Step 10 Enable or disable the policy by clicking the corresponding button in the **Operation** column. You can click ⟳ to refresh the page.

----End

Applying a Policy Group

Step 1 Log in to the management console and go to the HSS page.

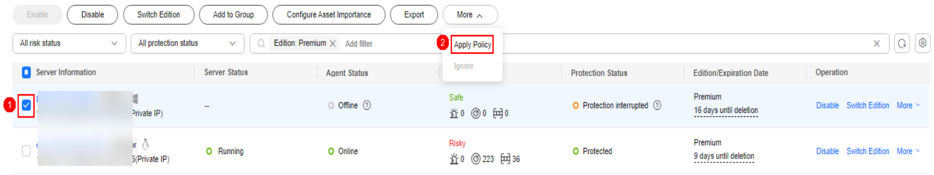
Step 2 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The **Servers** tab is displayed.

Step 3 Select one or more servers for which you want to deploy a policy, and click **More** > **Apply Policy**.

NOTE

After protection is enabled for a server, the protection policy of the corresponding protection edition is deployed by default. For servers that use the premium and container editions, you can create and deploy different protection policies.

Figure 4-26 Applying a policy



Server Information	Server Status	Agent Status		Protection Status	Edition/Expiration Date	Operation
☑ [redacted] Private IP)	--	Offline	Safe 0 0 0	Protection interrupted	Premium 16 days until deletion	Disable Switch Edition More
□ [redacted] 5(Private IP)	Running	Online	Risky 0 223 36	Protected	Premium 9 days until deletion	Disable Switch Edition More

Step 4 In the dialog box that is displayed, select a policy group and click **OK**.

After the policy group is applied, click ⚙ in the upper right corner of the server list, select **Policy Group** in the **Custom Columns** area, and click **OK**. Then, you can view the policy group of a server in the server list.

NOTE

- Old policies applied to a server will become invalid if you apply new policies to the server.
- Policies are applied to the servers within 1 minute.
- Policies applied to offline servers will not take effect until the servers are online.
- In a deployed policy group, you can enable, disable, or modify policies.
- A policy group that has been deployed cannot be deleted.

----End

4.4.6 Managing Server Groups

To manage servers by group, you can create a server group and add servers to it.

You can check the numbers of servers, unsafe servers, and unprotected servers in a group.

Creating a Server Group

After creating a server group, you can add servers to the group for unified management.

Step 1 Log in to the management console.

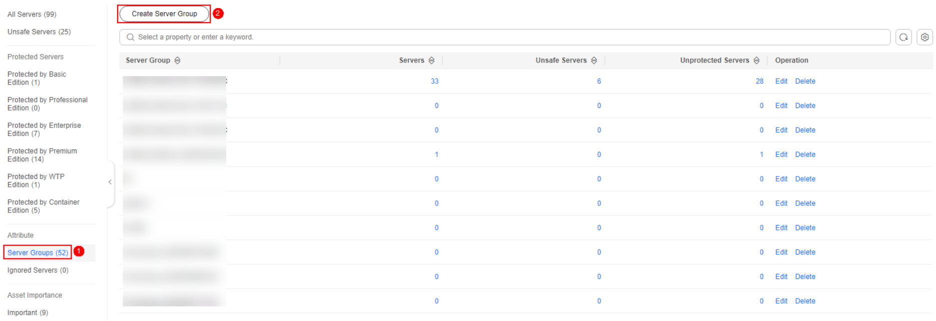
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 On the **Servers** tab page, click **Server Groups**, and click **Create Server Group**.

Figure 4-27 Accessing the page of server groups


All Servers (99)
Unsafe Servers (25)
Protected Servers
Protected by Basic Edition (1)
Protected by Professional Edition (0)
Protected by Enterprise Edition (7)
Protected by Premium Edition (14)
Protected by WTP Edition (1)
Protected by Container Edition (5)
Attribute
Server Groups (52)
1
Ignored Servers (0)
Asset Importance
Important (9)
Create Server Group
2
Select a property or enter a keyword.

Server Group	Servers	Unsafe Servers	Unprotected Servers	Operation
[redacted]	33	6	28	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	1	0	1	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete
[redacted]	0	0	0	Edit Delete

Step 6 In the **Create Server Group** dialog box, enter a server group name and select the servers to be added to the group.

- A server group name must be unique, or the group will fail to be created.
- A name cannot contain spaces. It contains only letters, digits, underscores (_), hyphens (-), dots (.), asterisks (*), and plus signs (+). The length cannot exceed 64 characters.

Step 7 Click **OK**.

----End

Adding Servers to Groups

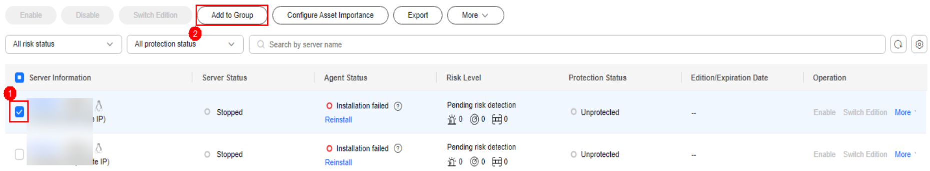
You can add servers to an existing server group. A server can be added to only one server group.

Step 1 Click the **Server** tab.

Step 2 Select one or more servers and click **Add to Group**.

To add a server to a group, you can also locate the row where the server resides, click **More** in the **Operation** column, and choose **Add to Group**.

Figure 4-28 Adding servers to a group



☐ Server Information	Server Status	Agent Status	Risk Level	Protection Status	Edition/Expiration Date	Operation
☑ [redacted] IP)	○ Stopped	Installation failed Reinstall	Pending risk detection 0 0 0	○ Unprotected	--	Enable Switch Edition More
☐ [redacted] te IP)	○ Stopped	Installation failed Reinstall	Pending risk detection 0 0 0	○ Unprotected	--	Enable Switch Edition More

Step 3 In the displayed dialog box, select a server group and click **OK**.

After the allocation is complete, click ⚙ in the upper right corner of the server list, select **Server Group** in the **Custom Columns** dialog box, and click **OK**. Then, you can view the group that a server belongs to in the server list.

----End

Related Operations

Editing a server group

Step 1 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the **Servers** tab, click **Server Groups**.

Step 2 Locate the row where a server group resides and click **Edit** in the **Operation** column.

Step 3 In the displayed dialog box, change the server group name and add or remove servers in the group.

Step 4 Click **OK**.

----End

Deleting a server group

Step 1 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the **Servers** tab, click **Server Groups**.

Step 2 Locate the row where a server group resides and click **Delete** in the **Operation** column.

NOTE

After the server group is deleted, the **Server Group** column of the servers that were in the group will be blank.

----End

4.4.7 Servers Importance Management

By default, HSS considers all servers as general assets. You can configure the asset importance levels of servers and manage servers accordingly.

Assets are classified into the following types:

- **Important**. Specify this level for servers that run important services or store important data.
- **General**. Specify this level for servers that run general services or store general data.
- **Test**. Specify this level for servers that run test services or store test data.

Checking Asset Importance

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The **Servers** tab is displayed.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the lower part of the tab page, check the asset importance. You can click **Important**, **General**, or **Test** to view servers by importance level.

----End

Specifying Asset Importance

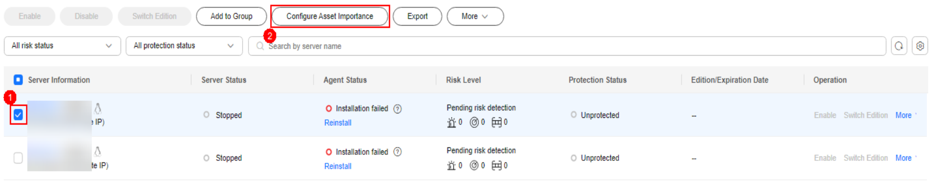
Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. The **Servers** tab is displayed.

Step 3 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 4 Select the target servers and click **Configure Asset Importance** above the list.

Figure 4-29 Configure Asset Importance



☑ Server Information	Server Status	Agent Status	Risk Level	Protection Status	Edition/Expiration Date	Operation
☑ [redacted] IP)	○ Stopped	○ Installation failed ⓘ Reinstall	Pending risk detection 0 0 0	○ Unprotected	--	Enable Switch Edition More
□ [redacted] te IP)	○ Stopped	○ Installation failed ⓘ Reinstall	Pending risk detection 0 0 0	○ Unprotected	--	Enable Switch Edition More

Step 5 In the dialog box that is displayed, select an asset importance level.

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

In the **Asset Importance** area in the lower left corner, select a level and check whether the importance of assets is correct.

----End

4.4.8 Ignoring a Server

You can ignore the servers that do not need to be protected. HSS will neither protect the ignored servers nor synchronize the information changes of the ignored servers.

Ignoring a Server

Step 1 Log in to the management console.

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

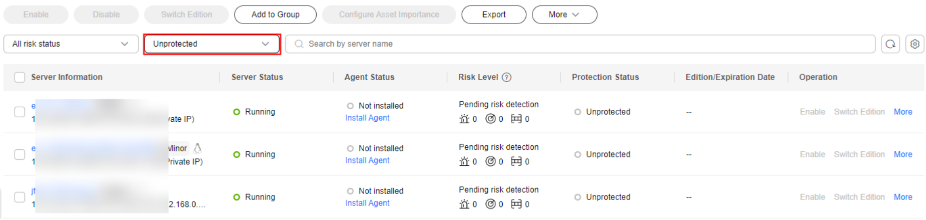
Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Servers** tab.

Step 6 Set filter criteria to filter unprotected servers.

Figure 4-30 Filtering unprotected servers

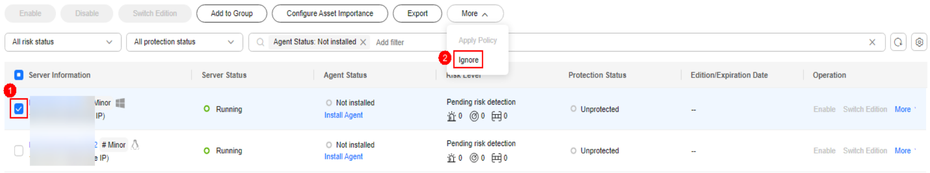


□ Server Information	Server Status	Agent Status	Risk Level ⓘ	Protection Status	Edition/Expiration Date	Operation
□ e 1 [redacted] /ate IP)	○ Running	○ Not installed Install Agent	Pending risk detection 0 0 0	○ Unprotected	--	Enable Switch Edition More
□ e 1 [redacted] Minor Private IP)	○ Running	○ Not installed Install Agent	Pending risk detection 0 0 0	○ Unprotected	--	Enable Switch Edition More
□ jf 1 [redacted] 2.168.0....	○ Running	○ Not installed Install Agent	Pending risk detection 0 0 0	○ Unprotected	--	Enable Switch Edition More

Step 7 Select the target server and click **More** > **Ignore** above the server list to ignore the server.

In the server type area on the left, click **Ignored Servers** under **Attribute** to view ignored servers.

Figure 4-31 Ignoring a server



☐ Server Information	Server Status	Agent Status	Risk Level	Protection Status	Edition/Expiration Date	Operation
☑ [redacted] Minor IP)	○ Running	○ Not installed Install Agent	Pending risk detection 0 0 0	○ Unprotected	--	Enable Switch Edition More
☐ [redacted] 2 # Minor e IP)	○ Running	○ Not installed Install Agent	Pending risk detection 0 0 0	○ Unprotected	--	Enable Switch Edition More

----End

Unignoring a Server

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

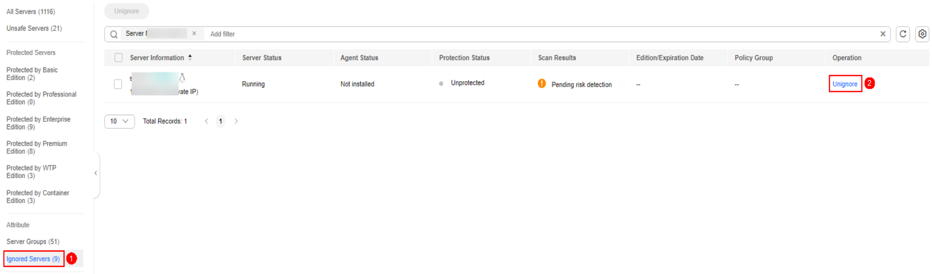
Step 5 Click the **Servers** tab.

Step 6 In the **Attribute** area, choose **Ignored Servers** to view the list of ignored servers.

Step 7 In the row of an ignored server, click **Unignore** in the **Operation** column.

At the top of the server type area on the left, click **All Servers**. You can view the unignored server in the server list.

Figure 4-32 Unignoring a server


All Servers (1116)
Unsafe Servers (21)
Protected Servers
Protected by Basic Edition (2)
Protected by Professional Edition (0)
Protected by Enterprise Edition (9)
Protected by Premium Edition (8)
Protected by WTP Edition (3)
Protected by Container Edition (3)
Attribute
Server Groups (51)
Ignored Servers (9)
1
Unignore
Server I [redacted]
Add filter
2
10
Total Records: 1
1

☐ Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Policy Group	Operation
☐ [redacted] ate IP)	Running	Not installed	● Unprotected	Pending risk detection	--	--	Unignore

----End

4.4.9 Disabling HSS

You can disable protection for a server. A quota that has been unbound from a server can be bound to another one.

Before You Start

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

To unsubscribe from the pay-per-use quota of a server, you just need to disable the protection.

Disabling HSS

The procedure for disabling protection varies depending on edition.

Disabling the Basic/Professional/Enterprise/Premium Edition

Step 1 Log in to the management console.

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

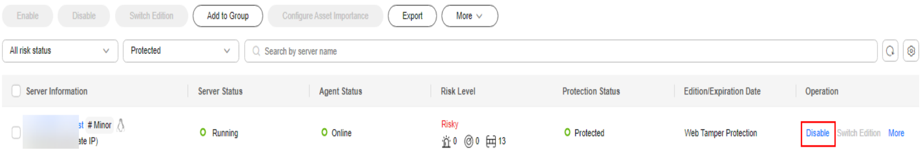
Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click **Disable** in the **Operation** column of a server.

You can also select multiple servers, and click **Disable** above the server list to disable protection in batches.

Figure 4-33 Disabling protection for a server



Server Information	Server Status	Agent Status	Risk Level	Protection Status	Edition/Expiration Date	Operation
st # Minor ate IP)	Running	Online	Risky 0 0 13	Protected	Web Tamper Protection	Disable Switch Edition More

Step 6 In the dialog box that is displayed, confirm the information and click **OK**.

Step 7 Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

----End

Disabling WTP

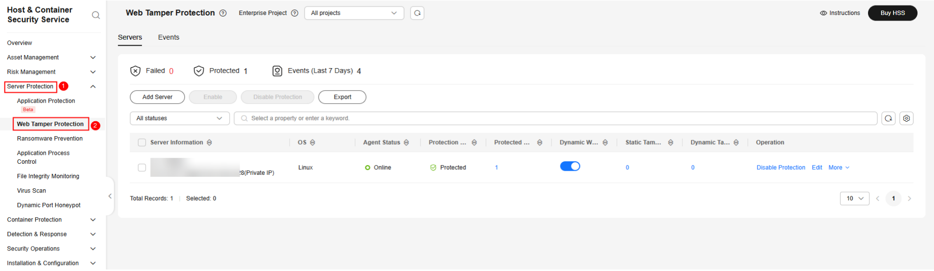
Disabling WTP stops protection and releases the protection quota (by unbinding the yearly/monthly quota or stopping the pay-per-use quota billing), but does not delete the configured WTP settings, such as protected directories and privileged processes.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Figure 4-34 Web tamper protection

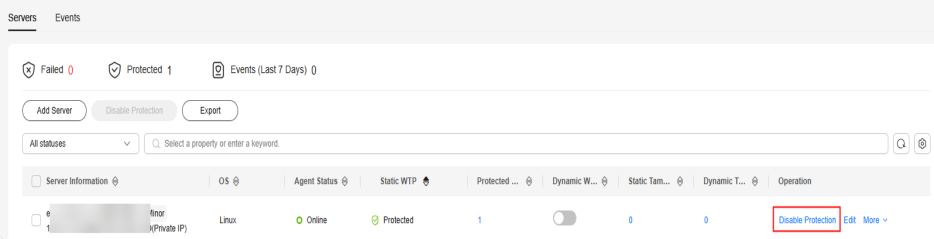


Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click **Disable** in the **Operation** column of a server.

You can also select multiple servers, and click **Disable** above the server list to disable protection in batches.

Figure 4-35 Disabling WTP



Step 6 In the dialog box that is displayed, confirm the information and click **OK**.

Step 7 Check the protection status of the server on the **Servers** tab. If it is **Unprotected**, the protection has been disabled.

NOTE

- To enable protection again, in the **Operation** column of a server, click **Enable**.
- If you have enabled dynamic WTP before disabling protection, you need to manually enable it after enabling protection again.

----End

4.5 Container Management

4.5.1 Viewing the Container Node Protection Status

The **Container Nodes** page displays the protection, node, and agent status of containers, helping you learn the node security status in real time.

Constraints

- Only Linux servers are supported.
- Servers that are not protected by HSS enterprise, premium, WTP, or container editions cannot perform container-related operations.

Viewing the Container Node Protection Status

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**. Click the **Container Nodes** tab.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View the node protection status. For details, see **Table 4-10**.

Table 4-10 Parameter description

Parameter	Description
Server Information	Server name and IP address. Move the cursor over to the server name to view the server details, including the server ID, OS, system name, and system version.
Protection Status	Protection status of a node. The options are as follows: ● **Unprotected**: HSS is disabled for the server. After the agent is installed, click **Enable** in the **Operation** column to enable protection. ● **Enabled**: The server is fully protected by HSS. ● **Protection interrupted**: The server is shut down, the agent is offline, or the agent is uninstalled.
Server Status	● Running ● Unavailable ● Normal

Parameter	Description
Agent Status	You can select a status to view the server. ● **Online**: The agent is running properly. ● **Offline**: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers. NOTE For an IDC server, its information will be automatically deleted from the node management page after its agent goes offline for 30 days. ● **Not installed**: The agent has not been installed or successfully started.

----End

4.5.2 Exporting the Container Node List

This section describes how to export the container node list to your local PC.

Exporting the Container Node List to the Local PC

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**. The container management page is displayed.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Choose the **Container Nodes** tab.

Step 6 In the upper part of the container list, click **Export** to export the list.

You can select multiple container nodes and click **Export** to export their container details in batches.

NOTE

The information about up to 1,000 container nodes can be exported at a time.

----End

4.5.3 Viewing Container Information

You can view container information on the **Containers** page to learn about the container status, cluster, and risks. This section describes how to view container information.

Constraints

Only the HSS container edition supports this function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.

Viewing Container Information

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

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

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**. The container management page is displayed.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Containers** tab. The container page is displayed.

Step 6 View the container information and security status.

In the container list, you can view the container name, status, risks, restart times, pod, and cluster name and type.

- View container details.

  Click the name of the target container. On the container details page that is displayed, view the container image, process, port, and mount path information.

- View the container risk distribution.

  View the number of low-risk, medium-risk, high-risk, and critical risks in the container.

- Export the container list.

  Click **Export** in the upper left corner of the list to export the container list to the local PC.

----End

4.5.4 Handling Unsafe Containers

Scenario

HSS can detect container security risks and classify them into the following types:

- Critical: malicious program
- High risk: ransomware attacks, malicious programs, reverse shells, escape attacks, and dangerous commands
- Medium risk: web shell, abnormal startup, process exception, and sensitive file access
- Low risk: brute-force attack

To prevent containers with medium or higher security risks from affecting other containers, you can isolate, suspend, or stop risky containers.

Constraints

- Only the HSS container edition supports this function. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading Your Edition**.
- Only Linux containers are supported.
- Only containers with medium or higher security risks can be handled.

Handling Unsafe Containers

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

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

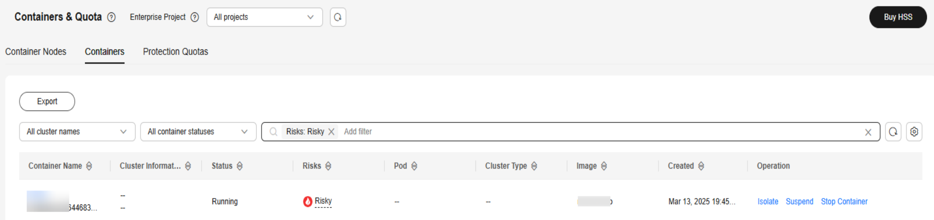
Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**. The container management page is displayed.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Containers** tab. The container page is displayed.

Step 6 In the search box above the container list, choose **Risks** > **Risky** to filter risky containers.

Figure 4-36 Filtering risky containers



Container Name	Cluster Informat...	Status	Risks	Pod	Cluster Type	Image	Created	Operation
[redacted]344683...	-- --	Running	Risky	--	--	[redacted]	Mar 13, 2025 19:45...	Isolate Suspend Stop Container

Step 7 In the **Operation** column of the target risky container, select the operation to be performed.

Only containers with medium or higher risks can be handled. You can view the security risk distribution. Cluster containers can be stopped. Independent containers can be isolated, suspended, and stopped.

- **Isolate containers**: After a container is isolated, you cannot access the container when the container is running, and the container cannot access the mount directory of the host or the system file of the container.
  a. Click **Isolate**.
  b. In the dialog box that is displayed, click **OK**.

     If the container status is **Isolated**, the operation succeeded.
- **Suspend containers**: Freeze the processes running in the container.

a. Click **Suspend**.

b. In the dialog box that is displayed, click **OK**.

If the container status is **Suspended**, the operation succeeded.

- **Stop containers**: Terminate a running container process. If **autoremove** is configured for the container, the container cannot be resumed.

a. Click **Stop Container**.

b. In the dialog box that is displayed, click **OK**.

If the container status is **Terminated**, the operation succeeded.

----End

Related Operations

Restoring a container to the running state

Restores a container from the **Isolate**, **Waiting**, or **Terminated** state to the **Running** state.

NOTE

If **autoremove** is configured for a terminated container, the container cannot be resumed.

Step 1 In the row containing the target container, click **Restore** in the **Operation** column.

Step 2 In the dialog box that is displayed, click **OK**.

----End

4.5.5 Uninstalling the Agent from a Cluster

After the uninstallation, some container-related functions, such as container firewall and container cluster protection, will be unavailable for the cluster assets connected to HSS through agents. To continue using container security services, you are advised to uninstall the cluster agent by following the instructions provided in this section, and then refer to **Installing an Agent in a Cluster** to connect to container assets again.

Uninstalling an Agent from a CCE Cluster

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

Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Containers** > **Cloud Container Engine**. The CCE console is displayed.

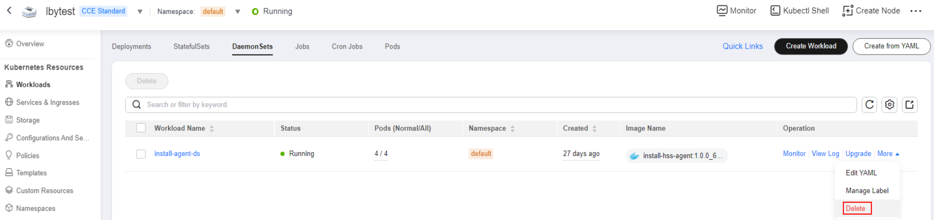
Step 3 Click the name of a cluster to enter its details page.

Step 4 In the navigation pane, choose **Workloads**.

Step 5 Click the **DaemonSets** tab. Delete the workload **install-agent-ds**.

In the **Operation** column of the workload, choose **More** > **Delete**.

Figure 4-37 Deleting install-agent-ds



Workload Name	Status	Pods (Normal/All)	Namespace	Created	Image Name	Operation
install-agent-ds	Running	4 / 4	default	27 days ago	install-hss-agent:1.0.0_6...	Monitor View Log Upgrade More

Step 6 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 7 In the navigation tree on the left, choose **Installation & Configuration** > **Server Install & Config**.

Step 8 Click the **Agents** tab. Uninstall the agent from all container nodes in the CCE cluster.

For details, see **Uninstalling the Agent**.

----End

Uninstalling an Agent from an On-Premises Cluster

Step 1 Log in to the Kubernetes cluster.

Step 2 Run the following command to delete the workload **install-agent-ds**:

kubectl delete ds install-agent-ds -n default

Step 3 **Log in to the management console**.

Step 4 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 5 In the navigation tree on the left, choose **Installation & Configuration** > **Server Install & Config**.

Step 6 Click the **Agents** tab. Uninstall the agent from all container nodes in the cluster.

For details, see **Uninstalling the Agent**.

----End

4.5.6 Disabling Container Protection

You can disable the container edition for a server. A quota that has been unbound from a server can be bound to another one.

Before You Start

- Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.
- To unsubscribe from the pay-per-use quota of the container edition, you just need to disable the protection.

Disabling the Container Edition

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**. Click the **Container Nodes** tab.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the **Operation** column of a server, click **Disable Protection**.

To disable protection in batches, select multiple target servers and click **Disable Protection**.

Step 6 In the dialog box that is displayed, confirm the information and click **OK**.

Step 7 After the function is disabled, choose **Asset Management** > **Containers & Quota**. On the **Container Nodes** tab, if the **Protection Status** of the server is **Unprotected**, it indicates protection has been disabled.

----End

4.6 Protection Quota Management

4.6.1 Viewing Protection Quotas

You can check, renew, and unsubscribe from your quota in the server list.

Only the quota purchased in the selected region is displayed. If your quota is not found, ensure you have switched to the correct region and search again.

Viewing Server Quotas

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 On the **Quotas** tab page, view HSS quotas. **Table 4-11** lists the related parameters.

Table 4-11 Parameter description

Parameter	Description
Quota ID	Unique ID of a quota. Click the quota ID to go to the basic information page. On this page, you can view the quota creation time, expiration policy, and last transaction order. You can also add tags to the quota on this page.
Edition	● Basic ● Professional Edition ● Enterprise ● Premium ● Web Tamper Protection (WTP)
Usage Status	● **In use**: The quota is being used for a server. The name of the server is displayed below the status. ● **Idle**: The quota is not in use.
Quota Status	● **Normal**: The quota has not expired and can be used properly. ● **Expired**: The quota has expired. During this period, you can still use the quota. ● **Frozen**: During the frozen period, the quota is unbound from the server and the server is no longer protected. After the frozen period expires, the quota is permanently deleted. If the quota expires and enters the frozen period, you can renew the quota in time, and the quota will be automatically bound to the original server (unless that server has been bound to another quota). If the quota is frozen due to public security reasons or violations, only after it is unbound by public security or violation management personnel, can it be automatically bound to the original server (unless that server has been bound to another quota).
Billing Mode	● Yearly/Monthly ● Pay-per-use
Enterprise Project Name	Name of the enterprise project to which the target quota belongs
Tag	Resource category tag.

NOTE

- Binding quota to a server

  Alternatively, choose **Asset Management** > **Servers & Quota** from the left navigation pane, and click the **Quotas** tab. In the quota list displayed, click **Bind Server** in the **Operation** column to bind a quota to a server. HSS will automatically protect the server.

  A quota can be bound to a server to protect it, on condition that the agent on the server is online.

- Unbind

  On the **Quotas** tab of the **Servers & Quota** page, click **Unbind** in the **Operation** column of a quota. HSS will no longer protect the server and the quota status will change to **Idle**.

- Export the quota list.

  Click ⧉ in the upper right corner of the quota list to export the quota information on the current page.

----End

Viewing Container Quotas

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Asset Management** > **Containers & Quota**. On the displayed page, click the **Protection Quotas** tab.

Step 4 On the **Protection Quotas** tab page, view HSS protection quotas. Table 4-12 lists the related parameters.

Table 4-12 Parameter description

Parameter	Description
Quota ID	Quota ID Click the quota ID to go to the basic information page. On this page, you can view the quota creation time, expiration policy, and last transaction order. You can also add tags to the quota on this page.
Quota Version	Enterprise edition
Quota Status	● **Normal**: The quota is normal. ● **Expired**: The quota has expired. During this period, you can still use the quota. ● **Frozen**: During the frozen period, the quota is unbound from the container node and the container node is no longer protected. If you renew the quota in time, the quota will be automatically bound to the container after the renewal is complete. After the frozen period expires, the quota will be permanently deleted.

Parameter	Description
Usage Status	- **In use**: The quota is being used for a server. The name of the server is displayed below the status. - **Idle**: The quota is not in use.
Billing Mode	- Yearly/Monthly - Pay-per-use
Tag	Resource category tag.

NOTE

- Renewal

  You can click **Renew** in the **Operation** column of the quota to renew it.For details, see **How Do I Renew HSS?**

- Unsubscription

  You can click **Unsubscribe** in the **Operation** column of the quota to unsubscribe from it. For details, see **How Do I Unsubscribe from HSS Quotas?**

----End

4.6.2 Binding a Protection Quota

You can bind a quota you purchased to a server to protect it.

Prerequisites

- The agent has been installed on the server, and the agent status is **Online**. For details about how to install the agent, see **Installing the Agent on Servers**.
- The quota is in **Normal** state and its **Usage Status** is **Idle**.
- A quota can be bound to a server to protect it, on condition that the agent on the server is online.

Manually Binding Quotas to a Server

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

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

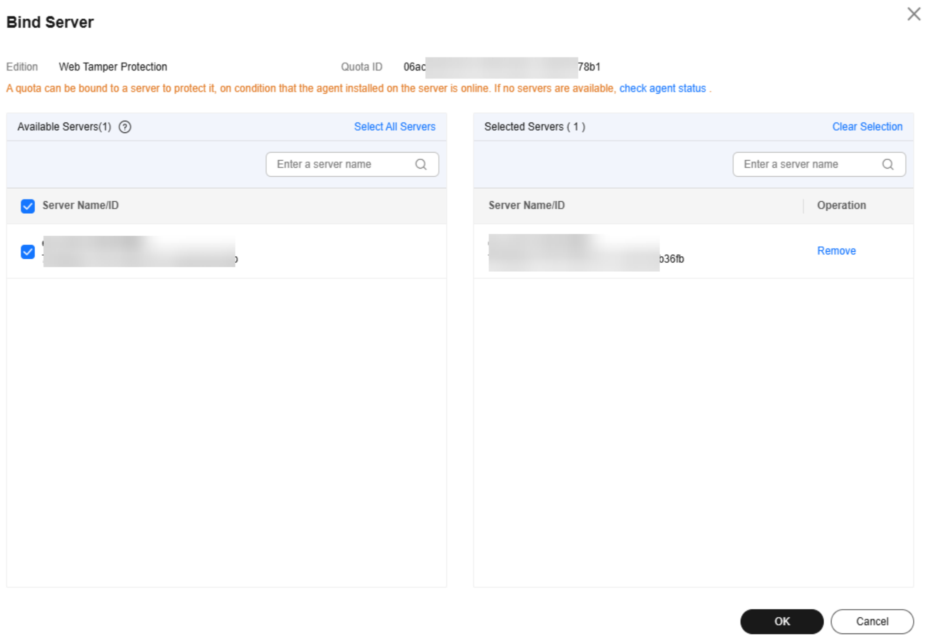
Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

Step 4 On the **Quotas** tab page, locate the row that contains the target quota and click **Bind Server** in the **Operation** column.

To bind a WTP quota to a server, choose **Server Protection** > **Web Tamper Protection** > **Servers** and click **Add Server**.

Step 5 Select a server.

Figure 4-38 Selecting a server to be bound



Bind Server

Edition Web Tamper Protection Quota ID 06ac[redacted]78b1

A quota can be bound to a server to protect it, on condition that the agent installed on the server is online. If no servers are available, check agent status .

Available Servers(1) ⓘ	Select All Servers
☑ Server Name/ID	
☑ [redacted]	

Selected Servers (1)	Clear Selection
Server Name/ID	Operation
[redacted]b36fb	Remove

Step 6 Click **OK**. HSS will automatically enable protection for the server.

----End

Manually Binding Quotas to a Container

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management** > **Containers & Quota**. Click the **Protection Quotas** tab. The protection quota list page is displayed.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 On the **Quotas** tab page, locate the row that contains the target quota and click **Bind Server** in the **Operation** column.

Step 6 Select a server.

Step 7 Click **OK**. HSS will automatically enable protection.

----End

Automatically Binding Quotas

Automatic Binding Description

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.

- 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.
- If the version of the agent installed on the Linux server is 3.2.10 or later or the version of the agent installed on the Windows server is 4.0.22 or later, ransomware prevention is automatically enabled with the premium, WTP, or container edition. Deploy honeypot files on servers and automatically isolate suspicious encryption processes (there is a low probability that processes are incorrectly isolated). You are also advised to enable backup so that you can restore data in the case of a ransomware attack to minimize losses. For details, see **Enabling Ransomware Backup**.

Procedure

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

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

Step 3 In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**.

NOTE

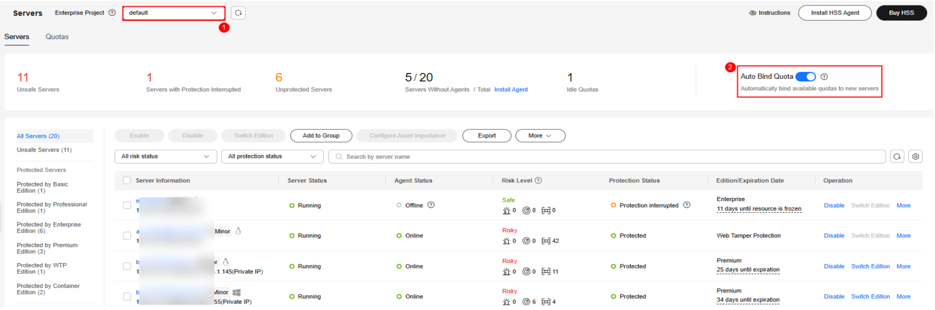
You can also configure the automatic quota binding function on either the protection quota purchasing page or the container management page.

Step 4 Perform the following operations based on whether enterprise projects are used:

- **Enterprise projects used**

  Select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page, and click ○ in the upper right corner of the **Servers** tab to enable automatic quota binding for the enterprise project.

Figure 4-39 Enabling automatic quota binding



Auto Bind Quota
Automatically bind available quotas to new servers

11	1	6	5 / 20	1
Unsafe Servers	Servers with Protection Interrupted	Unprotected Servers	Servers Without Agents / Total Install Agent	Idle Quotas

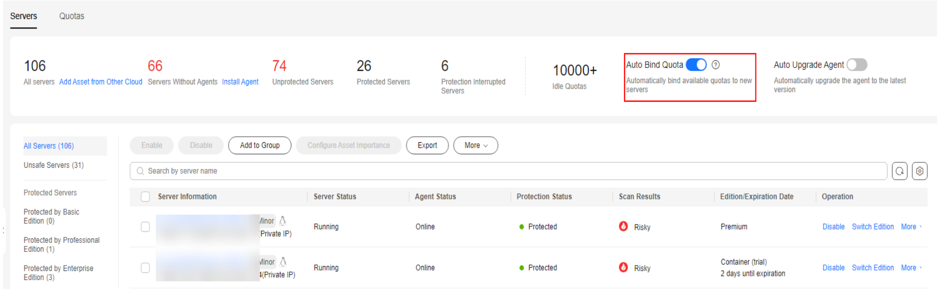
All Servers (20)
Unsafe Servers (11)
Protected Servers
Protected by Basic Edition (1)
Protected by Professional Edition (1)
Protected by Enterprise Edition (6)
Protected by Premium Edition (3)
Protected by WTP Edition (1)
Protected by Container Edition (2)

Server Information	Server Status	Agent Status	Risk Level	Protection Status	Edition/Expiration Date	Operation
[redacted]	Running	Offline	Safe 0 0 0	Protection interrupted	Enterprise 11 days until resource is frozen	Disable Switch Edition More
[redacted] Minor	Running	Online	Risky 0 0 42	Protected	Web Tamper Protection	Disable Switch Edition More
[redacted] .1.145(Private IP)	Running	Online	Risky 0 0 11	Protected	Premium 25 days until expiration	Disable Switch Edition More
[redacted] Minor 55(Private IP)	Running	Online	Risky 0 6 4	Protected	Premium 34 days until expiration	Disable Switch Edition More

- **No enterprise projects used**

Click in the upper right corner of the **Servers** tab to enable automatic quota binding.

Figure 4-40 Enabling automatic quota binding


Servers
Quotas
106
All servers
Add Asset from Other Cloud
66
Servers Without Agents
Install Agent
74
Unprotected Servers
26
Protected Servers
6
Protection Interrupted Servers
10000+
Idle Quotas
Auto Bind Quota
Automatically bind available quotas to new servers
Auto Upgrade Agent
Automatically upgrade the agent to the latest version
All Servers (106)
Unsafe Servers (31)
Protected Servers
Protected by Basic Edition (0)
Protected by Professional Edition (1)
Protected by Enterprise Edition (3)
Enable
Disable
Add to Group
Configure Asset Importance
Export
More
Search by server name

Server Information	Server Status	Agent Status	Protection Status	Scan Results	Edition/Expiration Date	Operation
[redacted] Minor Private IP)	Running	Online	● Protected	Risky	Premium	Disable Switch Edition More
[redacted] Minor (Private IP)	Running	Online	● Protected	Risky	Container (trial) 2 days until expiration	Disable Switch Edition More

----End

4.6.3 Unbinding a Protection Quota

You can unbind quotas from servers that no longer need to be protected. Exercise caution when performing this operation, because unprotected servers are exposed to security risks.

After unbinding a quota, you can bind it to another server or unsubscribe from it to reduce cost.

Prerequisites

The quotas to be unbound are in use.

Unbinding a Quota from a Server

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 On the **Quotas** page, click **Unbind** in the **Operation** column of a quota.

To unbind quotas in batches, select the servers they bind to, and click **Batch Unbind** above the quota list.

NOTE

Exercise caution when performing this operation, because unprotected servers are exposed to security risks.

Step 6 In the confirmation dialog box, click **OK**.

----End

Unbinding a Container Quota

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Asset Management** > **Containers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 On the **Quotas** page, click **Unbind** in the **Operation** column of a quota.

To unbind quotas in batches, select the servers they bind to, and click **Batch Unbind** above the quota list.

NOTE

Exercise caution when performing this operation, because unprotected servers are exposed to security risks.

Step 6 In the confirmation dialog box, click **OK**.

----End

4.6.4 Upgrading a Protection Quota

You can upgrade HSS from the basic or professional edition to a higher edition to enjoy stronger protection. For details, see **Table 4-13**.

Table 4-13 Quota upgrade plans

Current Edition	Supported Target Edition
Basic	Professional or premium
Professional	Premium

Premium, WTP, and container editions are high-configuration editions and cannot be upgraded. You can purchase these quotas separately. For details, see **Purchasing an HSS Quota**.

For details about the functions of each HSS edition, see **Features**.

Prerequisites

The **Usage Status** of a protection quota is **Idle**, and the **Quota Status** is **Normal**. If the quota has been bound to a server and its **Usage Status** is **In use**, **unbind the quota** before upgrade.

Upgrading a Quota

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

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

Step 3 In the navigation pane on the left, choose **Asset Management** > **Servers & Quota**. On the displayed page, click the **Quotas** tab. On the **Quotas** page, click the different option buttons to filter and view the target quota list.

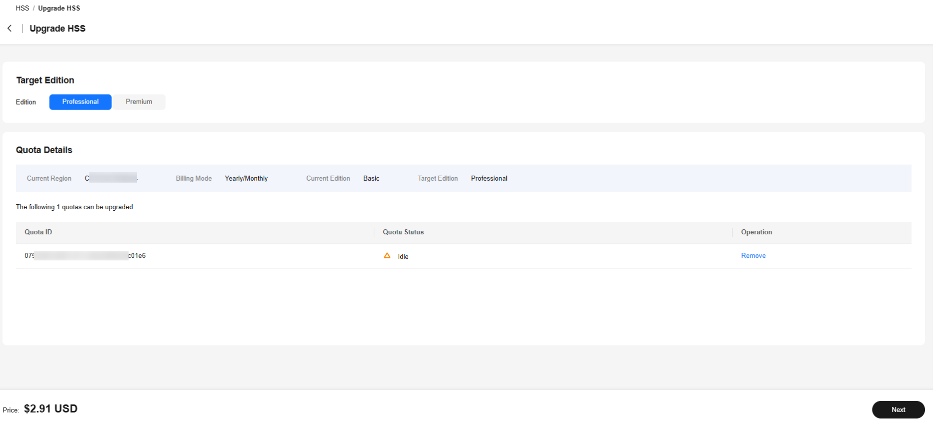
Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the quota list, filter the idle quotas of the basic or enterprise edition. Select a quota and click **Upgrade**.

Before upgrading a quota in use, **unbind it** from the server it protects.

Step 6 On the **Upgrade HSS** page, confirm the quota details and select a target edition.

Figure 4-41 Confirming upgrade information



HSS / Upgrade HSS

Upgrade HSS

Target Edition

Edition [✓ Professional] Premium

Quota Details

Current Region C[redacted] Billing Mode Yearly/Monthly Current Edition Basic Target Edition Professional

The following 1 quotas can be upgraded.

Quota ID	Quota Status	Operation
075[redacted]c01e6	Idle	Remove

Price: $2.91 USD

Next

Step 7 Confirm the upgrade specifications and click **Next**.

When you pay for the upgrade, you only need to make up the difference.

Step 8 On the **Pay** page, complete the payment.

Step 9 Wait until the payment is complete. Return to the quota list. Locate the quota by its ID and check its edition.

For details, see **Viewing Protection Quotas**.

Step 10 Wait until the upgrade succeeds. **Bind the quota to a server** and enable protection.

----End

4.6.5 Exporting the Protection Quota List

This section describes how to export the server protection quota list to your local PC. Currently, the container protection quota list cannot be exported.

Exporting the Protection Quota List

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Asset Management** > **Servers & Quota**.

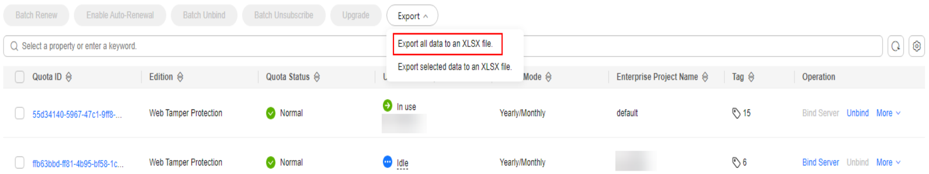
Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Quotas** tab.

Step 6 Above the protection quota list, click **Export** > **Export all data to an XLSX file** to export the server protection quota list.

If you only need to export specified protection quota information, select the target quota and choose **Export** > **Export selected data to an XLSX file**.

Figure 4-42 Exporting all server protection quotas


Batch Renew
Enable Auto-Renewal
Batch Unbind
Batch Unsubscribe
Upgrade
Export
Export all data to an XLSX file.
Export selected data to an XLSX file.
Select a property or enter a keyword.

□	Quota ID	Edition	Quota Status	U	Mode	Enterprise Project Name	Tag	Operation
□	55d34140-5967-47c1-9ff8-...	Web Tamper Protection	Normal	In use	Yearly/Monthly	default	15	Bind Server Unbind More
□	ffb63bbd-ff81-4b95-bf58-1c...	Web Tamper Protection	Normal	Idle	Yearly/Monthly		6	Bind Server Unbind More

Step 7 View the export status in the upper part of the page. After the export is successful, obtain the exported information from the default file download address on the local host.

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

5 Risk Management

5.1 Vulnerability Management

5.1.1 Vulnerability Management Overview

Vulnerability management can detect Linux, Windows, Web-CMS, application vulnerabilities, and emergency vulnerabilities and provide suggestions, helping you learn about server vulnerabilities in real time. Linux and Windows vulnerabilities can be fixed in one-click mode. This section describes how the vulnerabilities are detected and the vulnerabilities that can be scanned and fixed in each HSS edition.

NOTE

The vulnerability list displays vulnerabilities detected in the last seven days. After a vulnerability is detected for a server, if you change the server name and do not perform a vulnerability scan again, the vulnerability list still displays the original server name.

How Vulnerability Scan Works

Table 5-1 describes how different types of vulnerabilities are detected.

Table 5-1 How vulnerability scan works

Type	Mechanism
Linux vulnerability	Based on the vulnerability database, checks and handles vulnerabilities in the software (such as kernel, OpenSSL, vim, glibc) you obtained from official Linux sources and have not compiled, reports the results to the management console, and generates alarms.
Windows vulnerability	Synchronizes Microsoft official patches, checks whether the patches on the server have been updated, pushes Microsoft official patches, reports the results to the management console, and generates vulnerability alarms.

Type	Mechanism
Web-CMS vulnerability	Checks web directories and files for Web-CMS vulnerabilities, reports the results to the management console, and generates vulnerability alarms. Web-CMS vulnerability scans do not check network directories. The main reasons are as follows: 1. A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. 2. The access to network directories may occupy all your bandwidth and affect your services.
Application vulnerability	HSS detects the vulnerabilities in the software and dependency packages running on servers and container server machines, reports risky vulnerabilities to the console, and displays vulnerability alarms.
Emergency Vulnerabilities	Checks whether the software and any dependencies running on the server have vulnerabilities through version comparison and POC verification. Reports risky vulnerabilities to the console and provides vulnerability alarms for you.

Types of Vulnerabilities That Can Be Scanned and Fixed

For details about the types of vulnerabilities that can be scanned and fixed in different HSS editions, see **Types of vulnerabilities that can be scanned and fixed in each HSS edition**.

The meanings of the symbols in the table are as follows:

- √: supported
- ×: not supported

Table 5-2 Types of vulnerabilities that can be scanned and fixed in each HSS edition

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
Linux vulnerability	Automatic vulnerability scan (daily by default)	√	√	√	√	√	√

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	Scheduled vulnerability scan (once a week by default)	×	√	√	√	√	√
	Vulnerability whitelist	×	√	√	√	√	√
	Manual vulnerability scan	×	√	√	√	√	√
	One-click vulnerability fix	×	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√	√	√
Windows vulnerability	Automatic vulnerability scan (daily by default)	√	√	√	√	√	×
	Scheduled vulnerability scan (once a week by default)	×	√	√	√	√	×
	Vulnerability whitelist	×	√	√	√	√	×
	Manual vulnerability scan	×	√	√	√	√	×

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	One-click vulnerability fix	×	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√	√	×
Web-CMS vulnerability	Automatic vulnerability scan (daily by default)	×	√	√	√	√	√
	Scheduled vulnerability scan (once a week by default)	×	√	√	√	√	√
	Vulnerability whitelist	×	√	√	√	√	√
	Manual vulnerability scan	×	√	√	√	√	√
	One-click vulnerability fix	×	×	×	×	×	×
Application vulnerability	Automatic vulnerability scan (weekly by default)	×	×	√	√	√	√
	Scheduled vulnerability scan (once a week by default)	×	×	√	√	√	√

Vulnerability Type	Function	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	Vulnerability whitelist	×	×	√	√	√	√
	Manual vulnerability scan	×	×	√	√	√	√
	One-click vulnerability fix	×	×	×	×	×	×
Emergency vulnerability	Automatic vulnerability scan	×	×	×	×	×	×
	Scheduled vulnerability scan (disabled by default)	×	√	√	√	√	√
	Vulnerability whitelist	×	×	×	×	×	×
	Manual vulnerability scan	×	√	√	√	√	√
	One-click vulnerability fix	×	×	×	×	×	×

NOTE

HSS can scan for Web-CMS vulnerabilities, emergency vulnerabilities, and application vulnerabilities but cannot fix them. You can log in to your server to manually fix the vulnerability by referring to the suggestions displayed on the vulnerability details page.

5.1.2 Vulnerability Scan

HSS can scan for Linux, Windows, Web-CMS, application, and emergency vulnerabilities. Automatic, scheduled, and manual scans are supported.

- Automatic scan

  By default, Linux, Windows, and Web-CMS vulnerabilities are automatically scanned every day. Application vulnerabilities are automatically scanned every

Monday. The time of an automatic application vulnerability scan changes with the middleware asset scan time. For details about how to view and set the latter, see **Asset Discovery**.

If a manual or scheduled vulnerability scan has been performed in a day, HSS will not automatically scan for vulnerabilities on that day.

- Scheduled scan

  By default, a full server vulnerability scan is performed once a week. To protect workloads, you are advised to set a proper scan period and scan server scope to periodically scan server vulnerabilities.

- Manual scan

  If you want to view the vulnerability fixing status or real-time vulnerabilities of a server, you are advised to manually scan for vulnerabilities.

This section describes how to manually scan for vulnerabilities and configure a scheduled scan policy.

Constraints

- If the agent version of the Windows OS is 4.0.18 or later, application vulnerability scan is supported. If the agent version of the Linux OS is 3.2.9 or later, emergency vulnerability scan is supported. For details about how to upgrade the agent, see **Upgrading the Agent**.
- The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**. Otherwise, vulnerability scan cannot be performed.
- For details about the types of vulnerabilities that can be scanned by different HSS editions, see **Types of Vulnerabilities That Can Be Scanned and Fixed**.
- For details about the OSs supported by Linux and Windows vulnerability scan, see **Table 5-3**. Emergency vulnerability scan supports Ubuntu, CentOS, EulerOS, Debian, AlmaLinux, and Windows.

Table 5-3 OSs supporting vulnerability scan

OS Type	Supported OS
Windows	● Windows Server 2019 Datacenter 64-bit English (40 GB) ● Windows Server 2019 Datacenter 64-bit Chinese (40 GB) ● Windows Server 2016 Standard 64-bit English (40 GB) ● Windows Server 2016 Standard 64-bit Chinese (40 GB) ● Windows Server 2016 Datacenter 64-bit English (40 GB) ● Windows Server 2016 Datacenter 64-bit Chinese (40 GB) ● Windows Server 2012 R2 Standard 64-bit English (40 GB) ● Windows Server 2012 R2 Standard 64-bit Chinese (40 GB) ● Windows Server 2012 R2 Datacenter 64-bit English (40 GB) ● Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB) ● Windows Server 2022 Datacenter 64-bit English (40 GB) ● Windows Server 2022 Datacenter 64-bit Chinese (40 GB)

OS Type	Supported OS
Linux	● EulerOS 2.2, 2.3, 2.5, 2.8, 2.9, 2.10, 2.11, 2.12 (64-bit) ● CentOS 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 (64-bit) ● Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04 (64-bit) ● Debian 9, 10, and 11 (64-bit) ● Kylin V10, V10 SP1, and V10 SP2 (64-bit) ● HCE 1.1 and 2.0 (64-bit) ● SUSE 12 SP5, 15 SP1, and 15 SP2 (64-bit) ● UnionTech OS V20 server E, V20 server D, 1050u2e, 1050e, 1060e (64-bit) ● Rocky Linux 8.4, 8.5, 8.6, 8.10, 9.0, 9.1, 9.2, 9.4, and 9.5 (64-bit) ● OpenEuler 20.03, 22.03, and 24.03 (64-bit) ● CTyunOS 3-23.01 (64-bit) ● AlmaLinux 8.4 (64-bit)

Manual Vulnerability Scan

Step 1 Log in to the management console.

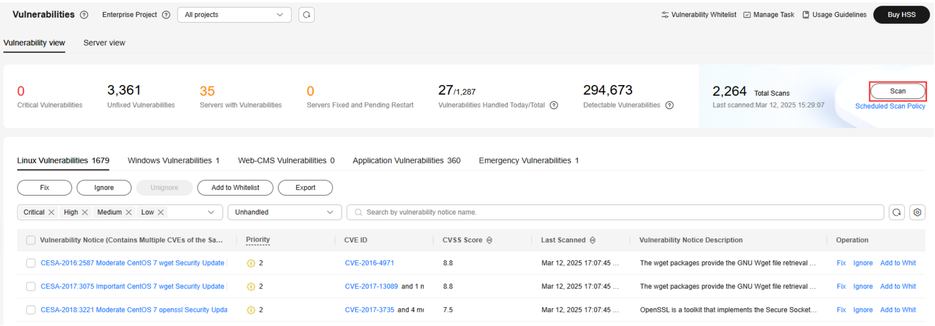
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 Click **Scan** in the upper right corner of the **Vulnerabilities** page.

To scan for emergency vulnerabilities, locate the row of an emergency vulnerability, and click **Scan** in the **Operation** column.

Figure 5-1 Manual scan

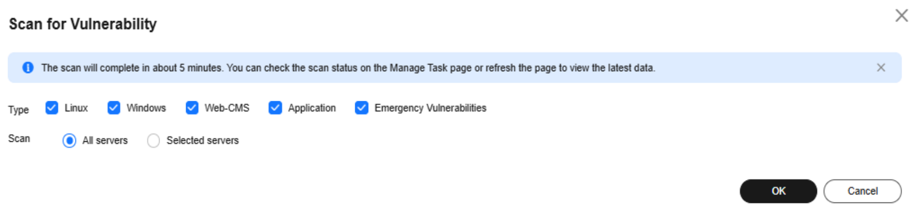


Vulnerabilities
Enterprise Project
All projects
Vulnerability Whitelist
Manage Task
Usage Guidelines
Buy HSS
Vulnerability view
Server view
0
Critical Vulnerabilities
3,361
Unfixed Vulnerabilities
35
Servers with Vulnerabilities
0
Servers Fixed and Pending Restart
27/1,287
Vulnerabilities Handled Today/Total
294,673
Detectable Vulnerabilities
2,264 Total Scans
Last scanned:Mar 12, 2025 15:29:07
Scan
Scheduled Scan Policy
Linux Vulnerabilities 1679
Windows Vulnerabilities 1
Web-CMS Vulnerabilities 0
Application Vulnerabilities 360
Emergency Vulnerabilities 1
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical
High
Medium
Low
Unhandled
Search by vulnerability notice name.

□ Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
□ CESA-2016:2587 Moderate CentOS 7 wget Security Update	2	CVE-2016-4971	8.8	Mar 12, 2025 17:07:45 ...	The wget packages provide the GNU Wget file retrieval ...	Fix Ignore Add to Whit
□ CESA-2017:3075 Important CentOS 7 wget Security Update	2	CVE-2017-13089 and 1 n	8.8	Mar 12, 2025 17:07:45 ...	The wget packages provide the GNU Wget file retrieval ...	Fix Ignore Add to Whit
□ CESA-2018:3221 Moderate CentOS 7 openssl Security Upda	2	CVE-2017-3735 and 4 m	7.5	Mar 12, 2025 17:07:45 ...	OpenSSL is a toolkit that implements the Secure Socket...	Fix Ignore Add to Whit

Step 5 In the **Scan for Vulnerability** dialog box displayed, set the vulnerability types and scope to be scanned. For more information, see **Table 5-4**.

Figure 5-2 Configuring a scan



Scan for Vulnerability

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

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

Scan ● All servers ○ Selected servers

Table 5-4 Parameters for manual scan vulnerabilities

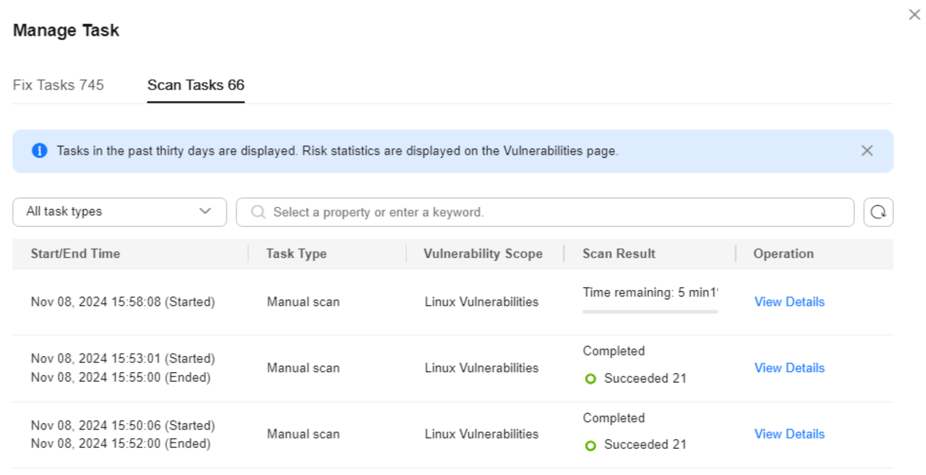
Parameter	Description	Example Value
Type	Select one or more types of vulnerabilities to be scanned. Possible values are as follows: ● **Linux** ● **Windows** ● **Web-CMS** ● **Application** ● **Emergency**	Select all
Scan	Select the servers to be scanned. Possible values are as follows: ● **All servers** ● **Selected servers** You can select a server group or search for the target server by server name, ID, EIP, or private IP address. The following servers cannot be selected for vulnerability scan: – Servers are protected by basic edition HSS. – Servers that are not in the **Running** state – Servers whose agent status is **Offline**	**All servers**

Step 6 Click **OK**.

Step 7 In the upper right corner of the **Vulnerabilities** page, click **Manage Task**, and click the **Scan Tasks** tab. View the scan task execution status.

In the **Operation** column of the target scan task, click **View Details** to view the scan details of a specific server.

Figure 5-3 Viewing scan tasks



Tasks in the past thirty days are displayed. Risk statistics are displayed on the Vulnerabilities page.

Start/End Time	Task Type	Vulnerability Scope	Scan Result	Operation
Nov 08, 2024 15:58:08 (Started)	Manual scan	Linux Vulnerabilities	Time remaining: 5 min1'	View Details
Nov 08, 2024 15:53:01 (Started) Nov 08, 2024 15:55:00 (Ended)	Manual scan	Linux Vulnerabilities	Completed ○ Succeeded 21	View Details
Nov 08, 2024 15:50:06 (Started) Nov 08, 2024 15:52:00 (Ended)	Manual scan	Linux Vulnerabilities	Completed ○ Succeeded 21	View Details

NOTE

You can also choose **Asset Management** > **Servers & Quota** and manually scan for vulnerabilities on a single server on the **Servers** tab page. The procedure is as follows:

1. Click a server name.
2. Choose **Vulnerabilities**.
3. Click the tab of a vulnerability type to be scanned and click **Scan**.

----End

Scheduled vulnerability scan

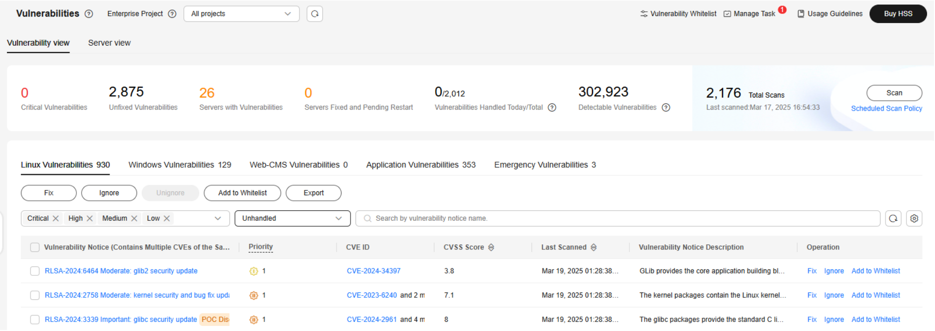
Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose Risk Management > **Vulnerabilities**.

Step 4 In the upper right corner of the **Vulnerabilities** page, click **Scheduled Scan Policy**. The **Configure Scheduled Scan Policy** dialog box is displayed.

Figure 5-4 Scheduled scan policy

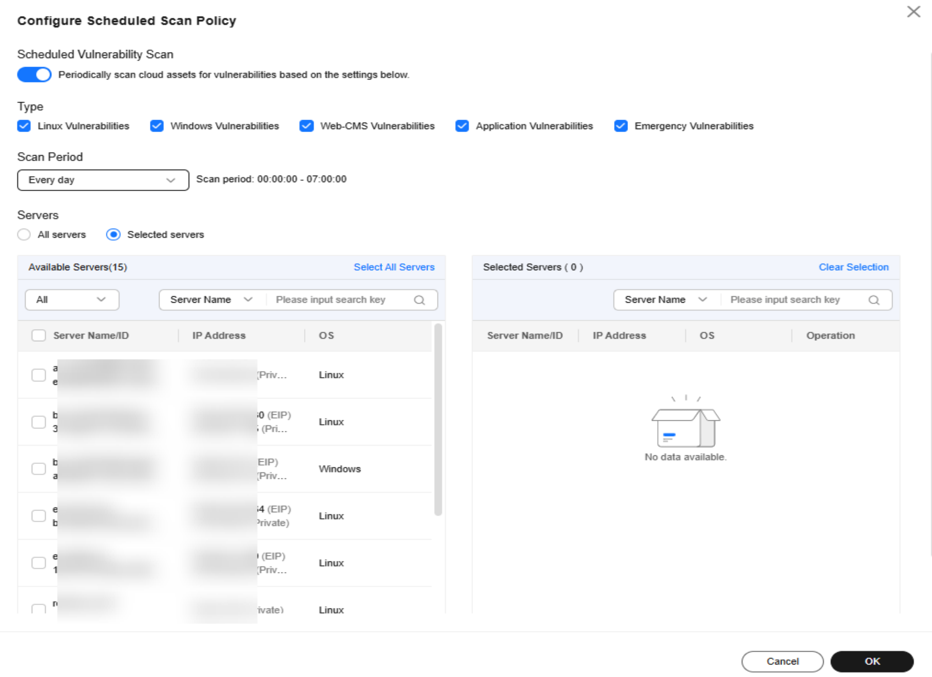


0 Critical Vulnerabilities
2,875 Unfixed Vulnerabilities
26 Servers with Vulnerabilities
0 Servers Fixed and Pending Restart
0/2,012 Vulnerabilities Handled Today/Total
302,923 Detectable Vulnerabilities
2,176 Total Scans
Last scanned:Mar 17, 2025 16:54:33

Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
RLSA-2024:6464 Moderate: glib2 security update	1	CVE-2024-34397	3.8	Mar 19, 2025 01:28:38...	GLib provides the core application building bl...	Fix Ignore Add to Whitelist
RLSA-2024:2758 Moderate: kernel security and bug fix upd	1	CVE-2023-6240 and 2 m	7.1	Mar 19, 2025 01:28:38...	The kernel packages contain the Linux kernel...	Fix Ignore Add to Whitelist
RLSA-2024:3339 Important: glibc security update POC Dis	1	CVE-2024-2961 and 4 m	8	Mar 19, 2025 01:28:38...	The glibc packages provide the standard C li...	Fix Ignore Add to Whitelist

Step 5 In the dialog box, configure parameters such as the period and scope for scheduled vulnerability scanning.

Figure 5-5 Configuring a scheduled scan policy



Configure Scheduled Scan Policy

Scheduled Vulnerability Scan

Periodically scan cloud assets for vulnerabilities based on the settings below.

Type

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

Scan Period

Every day — Scan period: 00:00:00 - 07:00:00

Servers

○ All servers ● Selected servers

Available Servers(15) — Select All Servers

□ Server Name/ID	IP Address	OS
a e [redacted]	[redacted] (Priv...	Linux
b 3 [redacted]	[redacted] 0 (EIP) (Pri...	Linux
b a [redacted]	[redacted] EIP) (Priv...	Windows
e b [redacted]	[redacted] 4 (EIP) Private)	Linux
e 1 [redacted]	[redacted] (EIP) (Priv...	Linux
r [redacted]	[redacted] ivate)	Linux

Selected Servers (0) — Clear Selection

Server Name/ID	IP Address	OS	Operation

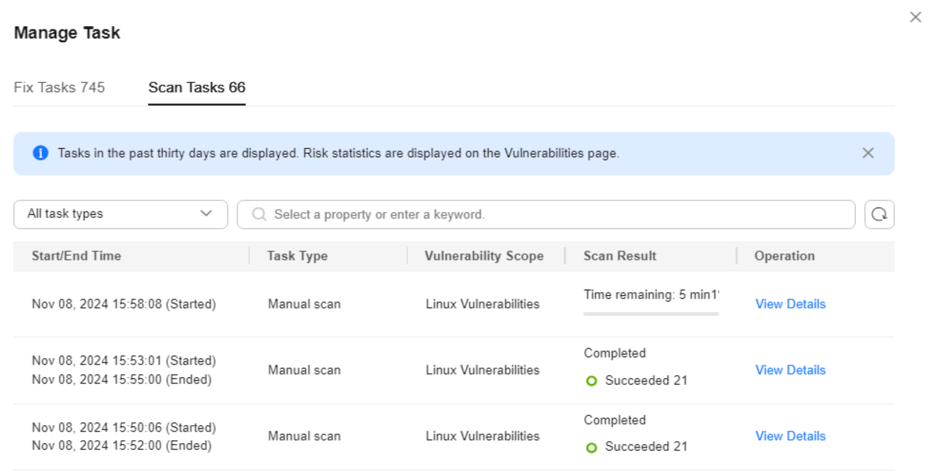
No data available.

- **Scheduled Vulnerability Scan**: Select whether to enable scheduled vulnerability scan. ● indicates it is enabled.
- **Type**: Select the types of vulnerabilities to be scanned.
- **Scan Period**: Select **Every day**, **Every three days**, or **Every week**. The default scan duration is **00:00:00 - 07:00:00** and cannot be changed.
- **Servers**: Select the server to be scanned. The following servers cannot be selected for vulnerability scan:
  - Servers that use the HSS basic edition
  - Servers that are not in the **Running** state
  - Servers whose agent status is **Offline**

Step 6 In the upper right corner of the **Vulnerabilities** page, click **Manage Task**, and click the **Scan Tasks** tab. View the scan task execution status.

In the **Operation** column of the target scan task, click **View Details** to view the scan details of a specific server.

Figure 5-6 Viewing scan tasks



Manage Task

Fix Tasks 745 | Scan Tasks 66

Tasks in the past thirty days are displayed. Risk statistics are displayed on the Vulnerabilities page.

All task types | Select a property or enter a keyword.

Start/End Time	Task Type	Vulnerability Scope	Scan Result	Operation
Nov 08, 2024 15:58:08 (Started)	Manual scan	Linux Vulnerabilities	Time remaining: 5 min1'	View Details
Nov 08, 2024 15:53:01 (Started) Nov 08, 2024 15:55:00 (Ended)	Manual scan	Linux Vulnerabilities	Completed ○ Succeeded 21	View Details
Nov 08, 2024 15:50:06 (Started) Nov 08, 2024 15:52:00 (Ended)	Manual scan	Linux Vulnerabilities	Completed ○ Succeeded 21	View Details

----End

FAQ

- **What Do I Do If a Vulnerability Scan Failed?**
- **Why Can't I Select a Server During Manual Vulnerability Scanning or Batch Vulnerability Fixing?**

5.1.3 Viewing Vulnerability Details

You can view vulnerabilities of your assets on the **Vulnerabilities** page. The **Vulnerabilities** page contains two tabs: **Vulnerabilities view** and **Server view**, helping you analyze vulnerabilities from the vulnerability and server perspectives.

Constraints

- Servers that are not protected by HSS do not support this function.
- The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**. Otherwise, vulnerability scan cannot be performed.

Viewing Vulnerability Details (Vulnerability View)

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

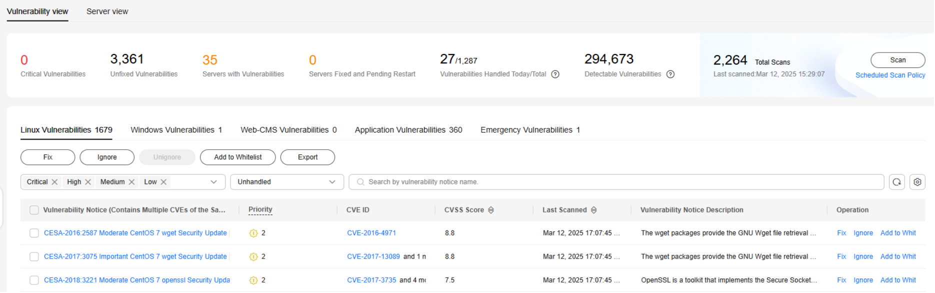
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View vulnerability information on the **Vulnerabilities** page.

Figure 5-7 Viewing vulnerability details


Vulnerability view
Server view
0
Critical Vulnerabilities
3,361
Unfixed Vulnerabilities
35
Servers with Vulnerabilities
0
Servers Fixed and Pending Restart
27/1,287
Vulnerabilities Handled Today/Total
294,673
Detectable Vulnerabilities
2,264 Total Scans
Last scanned:Mar 12, 2025 15:29:07
Scan
Scheduled Scan Policy
Linux Vulnerabilities 1679
Windows Vulnerabilities 1
Web-CMS Vulnerabilities 0
Application Vulnerabilities 360
Emergency Vulnerabilities 1
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical
High
Medium
Low
Unhandled
Search by vulnerability notice name.

Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
CESA-2016:2587 Moderate CentOS 7 wget Security Update	2	CVE-2016-4971	8.8	Mar 12, 2025 17:07:45 ...	The wget packages provide the GNU Wget file retrieval ...	Fix Ignore Add to Whit
CESA-2017:3075 Important CentOS 7 wget Security Update	2	CVE-2017-13089 and 1 n	8.8	Mar 12, 2025 17:07:45 ...	The wget packages provide the GNU Wget file retrieval ...	Fix Ignore Add to Whit
CESA-2018:3221 Moderate CentOS 7 openssl Security Upda	2	CVE-2017-3735 and 4 mi	7.5	Mar 12, 2025 17:07:45 ...	OpenSSL is a toolkit that implements the Secure Socket...	Fix Ignore Add to Whit

- Viewing vulnerability scan results

  In the vulnerability statistics area in the upper part of the **Vulnerabilities** page, view vulnerability scan results. **Table 5-5** describes related parameters.

  Table 5-5 Vulnerability scan parameters

Parameter	Description
Critical Vulnerabilities	Click the number in **Critical vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities to be urgently fixed.
Unfixed Vulnerabilities	Click the number in **Unfixed Vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities that are not fixed.
Servers with Vulnerabilities	Click the number in **Servers with Vulnerabilities**. You can view the servers with vulnerabilities in the lower part of the **Vulnerabilities** page.
Servers Fixed and Pending Restart	After Linux kernel vulnerabilities and Windows vulnerabilities are fixed, you need to restart the fixed servers. Otherwise, HSS will probably continue to warn you of these vulnerabilities. Click the number in the **Servers Fixed and Pending Restart** area to view the servers to be restarted.
Vulnerabilities Handled Today/ Total	Number of vulnerabilities handled today and the total number of vulnerabilities handled. You can click the numbers to view details. The total number of vulnerabilities is just the vulnerabilities handled within one year.
Detectable Vulnerabilities	Displays the number of vulnerabilities that can be detected by HSS.
Total Scans	Displays the number of vulnerability scans. Click **Scan** to manually scan for vulnerabilities on servers.

- Viewing vulnerability details

Click the name of a target vulnerability. On the vulnerability details slide-out panel displayed, you can view the repair suggestions, CVE details, affected servers, and historical handling records of the vulnerability.

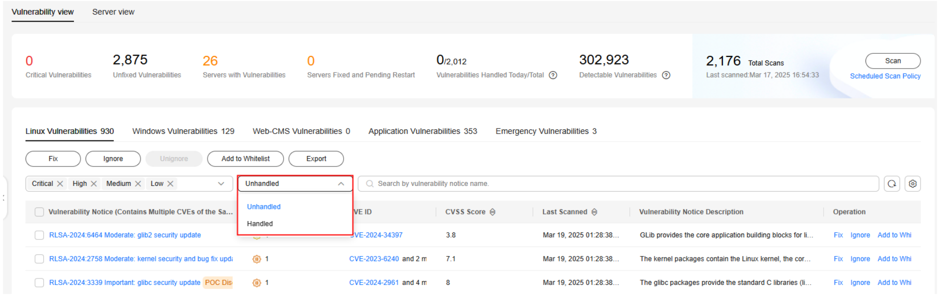
To check affected servers,

- Hover the cursor on the name of an affected server, and you can see the server status and OS version.
- If a server has the associated process, click the server name and check process details in the **Associated Process** column.

- Viewing handled vulnerabilities or vulnerabilities to be handled

  Above the vulnerability list, select **Unhandled** or **Handled** from the vulnerability handling status drop-down list to filter vulnerabilities.

Figure 5-8 Filtering handled or unhandled vulnerabilities



Vulnerability view | Server view

0 Critical Vulnerabilities | 2,875 Unfixed Vulnerabilities | 26 Servers with Vulnerabilities | 0 Servers Fixed and Pending Restart | 0/2,012 Vulnerabilities Handled Today/Total | 302,923 Detectable Vulnerabilities | 2,176 Total Scans Last scanned:Mar 17, 2025 16:54:33

Scan | Scheduled Scan Policy

Linux Vulnerabilities 930 | Windows Vulnerabilities 129 | Web-CMS Vulnerabilities 0 | Application Vulnerabilities 353 | Emergency Vulnerabilities 3

Fix | Ignore | Unignore | Add to Whitelist | Export

Critical × High × Medium × Low × | Unhandled (Unhandled, Handled) | Search by vulnerability notice name.

Vulnerability Notice (Contains Multiple CVEs of the Sa...		VE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
RLSA-2024:6464 Moderate: glib2 security update		VE-2024-34397	3.8	Mar 19, 2025 01:28:38...	GLib provides the core application building blocks for li...	Fix Ignore Add to Whi
RLSA-2024:2758 Moderate: kernel security and bug fix upd	1	CVE-2023-6240 and 2 m	7.1	Mar 19, 2025 01:28:38...	The kernel packages contain the Linux kernel, the cor...	Fix Ignore Add to Whi
RLSA-2024:3339 Important: glibc security update POC Dis	1	CVE-2024-2961 and 4 m	8	Mar 19, 2025 01:28:38...	The glibc packages provide the standard C libraries (li...	Fix Ignore Add to Whi

----End

Viewing Vulnerability Details (Server View)

The basic edition does not provide the server view.

Step 1 Log in to the management console.

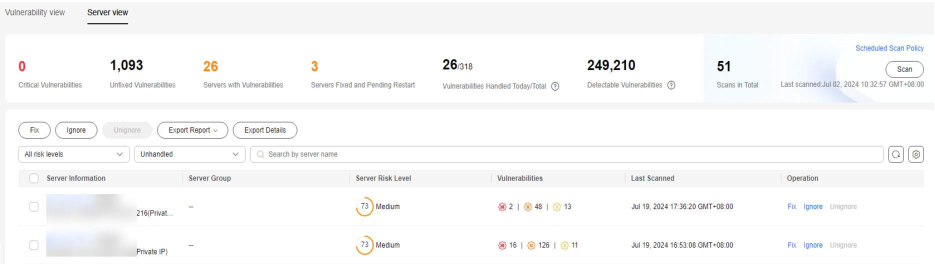
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the upper left corner of the **Vulnerabilities** page, click **Server view** to view vulnerability information.

Figure 5-9 Viewing vulnerability details



Vulnerability view | Server view

0 Critical Vulnerabilities | 1,093 Unfixed Vulnerabilities | 26 Servers with Vulnerabilities | 3 Servers Fixed and Pending Restart | 26/318 Vulnerabilities Handled Today/Total | 249,210 Detectable Vulnerabilities | 51 Scans in Total

Scheduled Scan Policy | Scan | Last scanned:Jul 02, 2024 10:32:57 GMT+08:00

Fix | Ignore | Unignore | Export Report | Export Details

All risk levels | Unhandled | Search by server name

Server Information	Server Group	Server Risk Level	Vulnerabilities	Last Scanned	Operation
[redacted]216(Privat...	--	73 Medium	2 | 48 | 13	Jul 19, 2024 17:36:20 GMT+08:00	Fix Ignore Unignore
[redacted]Private IP)	--	73 Medium	16 | 126 | 11	Jul 19, 2024 16:53:08 GMT+08:00	Fix Ignore Unignore

- Viewing vulnerability scan results

  In the vulnerability statistics area in the upper part of the **Vulnerabilities** page, view vulnerability scan results. **Table 5-6** describes related parameters.

Table 5-6 Vulnerability scan parameters

Parameter	Description
Critical Vulnerabilities	Click the number in **Critical vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities to be urgently fixed.
Unfixed Vulnerabilities	Click the number in **Unfixed Vulnerabilities**. On the slide-out panel displayed, you can view all types of vulnerabilities that are not fixed.
Servers with Vulnerabilities	Click the number in **Servers with Vulnerabilities**. You can view the servers with vulnerabilities in the lower part of the **Vulnerabilities** page.
Servers Fixed and Pending Restart	After Linux kernel vulnerabilities and Windows vulnerabilities are fixed, you need to restart the fixed servers. Otherwise, HSS will probably continue to warn you of these vulnerabilities. Click the number in the **Servers Fixed and Pending Restart** area to view the servers to be restarted.
Vulnerabilities Handled Today/ Total	Number of vulnerabilities handled today and the total number of vulnerabilities handled. You can click the numbers to view details. The total number of vulnerabilities is just the vulnerabilities handled within one year.
Detectable Vulnerabilities	Displays the number of vulnerabilities that can be detected by HSS.
Total Scans	Displays the number of vulnerability scans. Click **Scan** to manually scan for vulnerabilities on servers.

- Viewing server details and vulnerabilities on servers

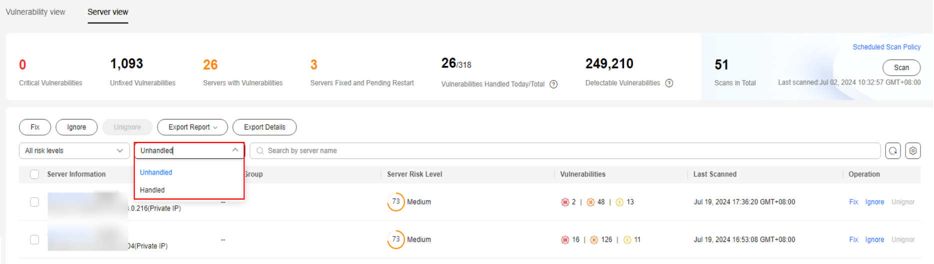
  a. Click the name of a target server. On the server details slide-out panel displayed, you can view details about the server and vulnerabilities on the server.

  b. Click the name of a target vulnerability. On the vulnerability details slide-out panel displayed, you can view the CVE details, affected servers, and historical handling records of the vulnerability.

- Viewing handled vulnerabilities or vulnerabilities to be handled

  Above the vulnerability list, select **Unhandled** or **Handled** from the vulnerability handling status drop-down list to filter vulnerabilities to be handled or that have been handled.

Figure 5-10 Filtering handled or unhandled vulnerabilities



Server Information	Group	Server Risk Level	Vulnerabilities	Last Scanned	Operation
[redacted] .0.216(Private IP)	--	73 Medium	2 | 48 | 13	Jul 19, 2024 17:36:20 GMT+08:00	Fix Ignore Unignor
[redacted] 04(Private IP)	--	73 Medium	16 | 126 | 11	Jul 19, 2024 16:53:08 GMT+08:00	Fix Ignore Unignor

----End

5.1.4 Exporting the Vulnerability List

You can refer to this section to export the vulnerability list.

Prerequisite

The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**. For details, see **Viewing Server Protection Status**.

Constraints

This function is available in HSS professional, enterprise, premium, WTP, and container editions.

Exporting the Vulnerability List (Vulnerability View)

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

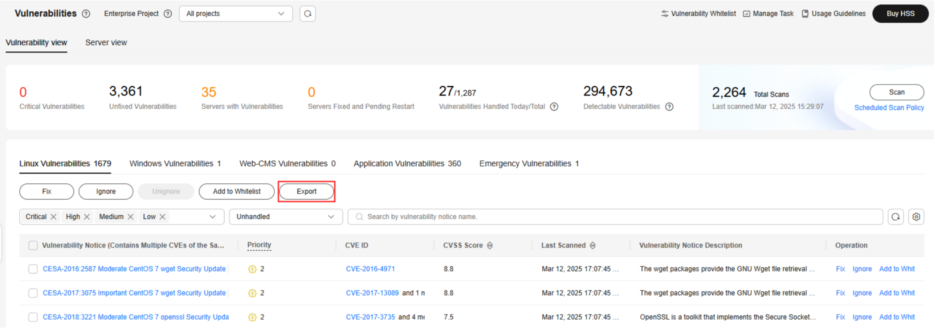
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 In the upper left corner of the **Vulnerabilities** page, click the **Vulnerability view** tab.

Step 5 Click **Export** above the vulnerability list to export the vulnerability list.

Figure 5-11 Exporting the vulnerability list


Vulnerabilities
Enterprise Project
All projects
Vulnerability Whitelist
Manage Task
Usage Guidelines
Buy HSS
Vulnerability view
Server view
0
Critical Vulnerabilities
3,361
Unfixed Vulnerabilities
35
Servers with Vulnerabilities
0
Servers Fixed and Pending Restart
27/1,287
Vulnerabilities Handled Today/Total
294,673
Detectable Vulnerabilities
2,264 Total Scans
Last scanned:Mar 12, 2025 15:29:07
Scan
Scheduled Scan Policy
Linux Vulnerabilities 1679
Windows Vulnerabilities 1
Web-CMS Vulnerabilities 0
Application Vulnerabilities 360
Emergency Vulnerabilities 1
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical
High
Medium
Low
Unhandled
Search by vulnerability notice name.

Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
CESA-2016:2587 Moderate CentOS 7 wget Security Update	2	CVE-2016-4971	8.8	Mar 12, 2025 17:07:45 ...	The wget packages provide the GNU Wget file retrieval ...	Fix Ignore Add to Whit
CESA-2017:3075 Important CentOS 7 wget Security Update	2	CVE-2017-13089 and 1 n	8.8	Mar 12, 2025 17:07:45 ...	The wget packages provide the GNU Wget file retrieval ...	Fix Ignore Add to Whit
CESA-2018:3221 Moderate CentOS 7 openssl Security Upda	2	CVE-2017-3735 and 4 m	7.5	Mar 12, 2025 17:07:45 ...	OpenSSL is a toolkit that implements the Secure Socket...	Fix Ignore Add to Whit

Step 6 View the export status in the upper part of the **Vulnerabilities** page. After the export is successful, obtain the exported information from the default file download address on the local host.

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

Exporting the Vulnerability List (Server View)

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

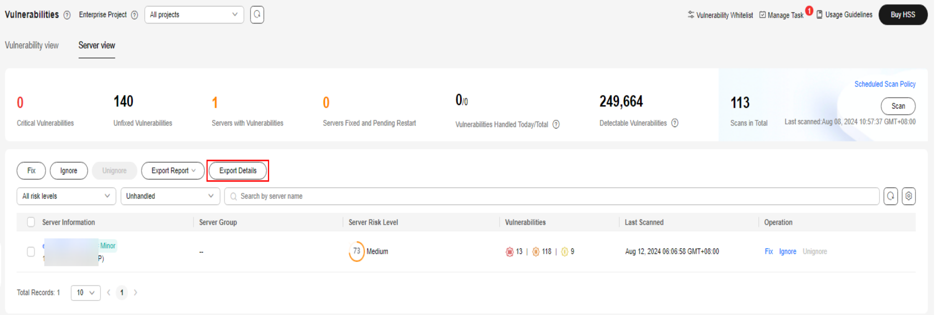
Step 4 In the upper left corner of the **Vulnerabilities** page, click the **Server view** tab.

Step 5 Export the vulnerability list.

- Export vulnerability details: In the upper part of the vulnerability list, click **Export Details** to export the vulnerability list.

  You can select the risk level, vulnerability handling status, or search criteria to filter the vulnerability information of the target server, and click **Export Details** to export the vulnerability details.

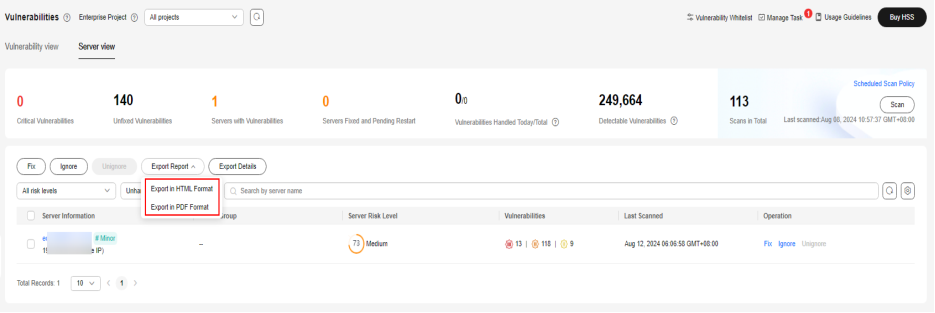
  Figure 5-12 Exporting vulnerability details



Server Information	Server Group	Server Risk Level	Vulnerabilities	Last Scanned	Operation
[redacted] Minor P)	--	73 Medium	13 | 118 | 9	Aug 12, 2024 06:06:58 GMT+08:00	Fix Ignore Unignore

- Export a vulnerability report: In the upper part of the vulnerability list, click **Export Report** and select a report format.
  - When exporting a vulnerability report in HTML format, the vulnerability information about up to 100 servers can be exported. In the exported HTML vulnerability report, you can view vulnerability details.
  - When exporting a vulnerability report in PDF format, the vulnerability information about up to 140 servers and vulnerabilities can be exported.
  - To export vulnerability reports of some servers, you can select the servers and click **Export**.

Figure 5-13 Exporting a vulnerability report



Step 6 View the export status in the upper part of the **Vulnerabilities** page. After the export is successful, obtain the exported information from the default file download address on the local host.

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

5.1.5 Handling Vulnerabilities

If HSS detects a vulnerability on a server, you need to handle the vulnerability in a timely manner based on its severity and your business conditions to prevent the vulnerability from being exploited by intruders.

Vulnerabilities can be handled in the following ways. For details, see **Handling Vulnerabilities**.

- **Fixing vulnerabilities**

  If a vulnerability may harm your services, fix it as soon as possible. For Linux and Windows vulnerabilities, you can let HSS fix them in one-click. Web-CMS vulnerabilities, emergency vulnerabilities, and application vulnerabilities cannot be automatically fixed. Handle them by referring to the suggestions provided on the vulnerability details page.
- **Ignoring vulnerabilities**

  Some vulnerabilities are risky only in specific conditions. For example, if a vulnerability can be exploited only through an open port, but the target server does not open any ports, the vulnerability will not harm the server. If you can confirm that a vulnerability is harmless, you can ignore it.
- **Adding vulnerabilities to the whitelist**

  If you can confirm that a vulnerability does not affect your services and does not need to be fixed, you can add it to the whitelist. After a vulnerability is added to the whitelist, its status will change to **Ignored** in the vulnerability list, and it will not be reported in later scans.

Constraints

- For details about vulnerability handling operations supported by each HSS version, see **Types of Vulnerabilities That Can Be Scanned and Fixed**.
- CentOS 7, CentOS 8, Debian 9 and 10, Windows 2012 R2, and Ubuntu 14.04 and earlier have reached EOL and cannot be fixed because no official patches are available. You are advised to change to the OSs in active support.

- Ubuntu 16.04 to Ubuntu 22.04 do not support certain free patch updates. You need to subscribe to Ubuntu Pro to install upgrade packages. If Ubuntu Pro is not configured, vulnerabilities will fail to be fixed. For details about the vulnerabilities that need to be fixed by subscribing to Ubuntu Pro, see **Do I Need to Subscribe to Ubuntu Pro to Fix Ubuntu Vulnerabilities?**
- Fixing kernel vulnerabilities may cause servers to be unavailable. Therefore, HSS does not automatically fix the server kernel vulnerabilities of CCE, MRS, or BMS. When batch fixing vulnerabilities, HSS filters out these types of vulnerabilities.
- To handle vulnerabilities on a server, ensure the server is in the **Running** state, its agent status is **Online**, and its protection status is **Protected**.
- A maximum of 2000 vulnerabilities can be added to the whitelist.

Precautions

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

Vulnerability Fix Priority

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

NOTE

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

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

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

- **Medium**: You are advised to fix the vulnerability to enhance your server security.
- **Low**: This vulnerability has a small threat to server security. You can choose to fix or ignore it.

Vulnerability Display

Detected vulnerabilities will be displayed in the vulnerability list for seven days, regardless of whether you have handled them.

Handling Vulnerabilities

You can handle the vulnerability in following ways: After a vulnerability is handled, its status changes to **Handled**. You can select **Handled** or **Unhandled** above the list to view vulnerabilities or servers in the corresponding status.

Automatically Fixing Vulnerabilities (Vulnerability View)

You can only fix Linux and Windows vulnerabilities with one-click on the console. A maximum of 1,000 server vulnerabilities can be fixed at a time. If there are more than 1,000 vulnerabilities, fix them in batches.

Step 1 Log in to the management console.

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

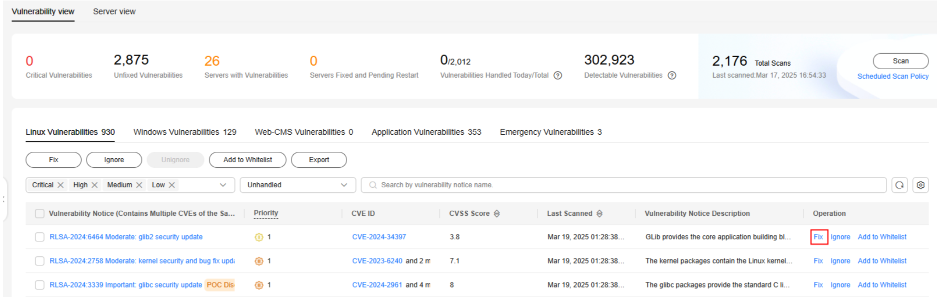
Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 Fix Linux and Windows vulnerabilities.

- Fixing a single vulnerability

  Locate the row containing a target vulnerability and click **Fix** in the **Operation** column.

Figure 5-14 Fixing a single vulnerability

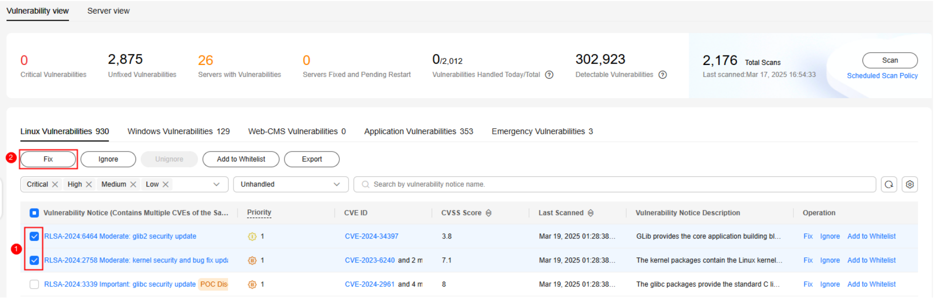

Vulnerability view
Server view
0
Critical Vulnerabilities
2,875
Unfixed Vulnerabilities
26
Servers with Vulnerabilities
0
Servers Fixed and Pending Restart
0/2,012
Vulnerabilities Handled Today/Total
302,923
Detectable Vulnerabilities
2,176 Total Scans
Last scanned:Mar 17, 2025 16:54:33
Scan
Scheduled Scan Policy
Linux Vulnerabilities 930
Windows Vulnerabilities 129
Web-CMS Vulnerabilities 0
Application Vulnerabilities 353
Emergency Vulnerabilities 3
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical
High
Medium
Low
Unhandled
Search by vulnerability notice name.

☐ Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
☐ RLSA-2024:6464 Moderate: glib2 security update	1	CVE-2024-34397	3.8	Mar 19, 2025 01:28:38...	GLib provides the core application building bl...	Fix Ignore Add to Whitelist
☐ RLSA-2024:2758 Moderate: kernel security and bug fix upd	1	CVE-2023-6240 and 2 m	7.1	Mar 19, 2025 01:28:38...	The kernel packages contain the Linux kernel...	Fix Ignore Add to Whitelist
☐ RLSA-2024:3339 Important: glibc security update POC Dis	1	CVE-2024-2961 and 4 m	8	Mar 19, 2025 01:28:38...	The glibc packages provide the standard C li...	Fix Ignore Add to Whitelist

- Fixing multiple vulnerabilities

  Select all target vulnerabilities and click **Fix** in the upper left corner of the vulnerability list to fix vulnerabilities in batches.

Figure 5-15 Fixing multiple vulnerabilities


Vulnerability view
Server view
Scan
Scheduled Scan Policy
Linux Vulnerabilities 930
Windows Vulnerabilities 129
Web-CMS Vulnerabilities 0
Application Vulnerabilities 353
Emergency Vulnerabilities 3
2
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical
High
Medium
Low
Unhandled
Search by vulnerability notice name.
1

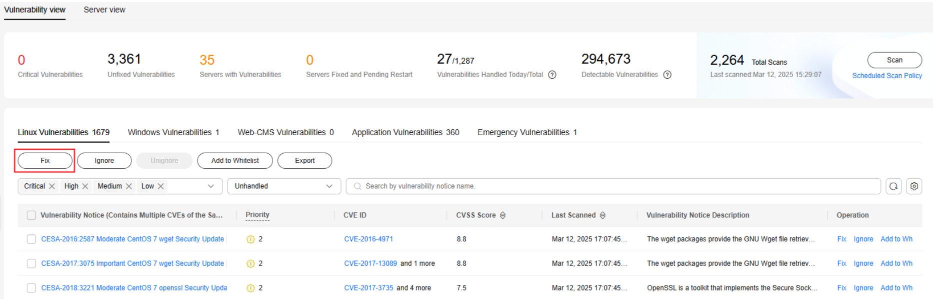
0 Critical Vulnerabilities | 2,875 Unfixed Vulnerabilities | 26 Servers with Vulnerabilities | 0 Servers Fixed and Pending Restart | 0/2,012 Vulnerabilities Handled Today/Total | 302,923 Detectable Vulnerabilities | 2,176 Total Scans, Last scanned:Mar 17, 2025 16:54:33

☑ Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
☑ RLSA-2024:6464 Moderate: glib2 security update	1	CVE-2024-34397	3.8	Mar 19, 2025 01:28:38...	GLib provides the core application building bl...	Fix Ignore Add to Whitelist
☑ RLSA-2024:2758 Moderate: kernel security and bug fix upd:	1	CVE-2023-6240 and 2 m	7.1	Mar 19, 2025 01:28:38...	The kernel packages contain the Linux kernel...	Fix Ignore Add to Whitelist
□ RLSA-2024:3339 Important: glibc security update POC Dis	1	CVE-2024-2961 and 4 m	8	Mar 19, 2025 01:28:38...	The glibc packages provide the standard C li...	Fix Ignore Add to Whitelist

- Fix all vulnerabilities.

  Click **Fix** in the upper left corner of the vulnerability list to fix all vulnerabilities.

Figure 5-16 Fixing all vulnerabilities


Vulnerability view
Server view
Scan
Scheduled Scan Policy
Linux Vulnerabilities 1679
Windows Vulnerabilities 1
Web-CMS Vulnerabilities 0
Application Vulnerabilities 360
Emergency Vulnerabilities 1
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical
High
Medium
Low
Unhandled
Search by vulnerability notice name.

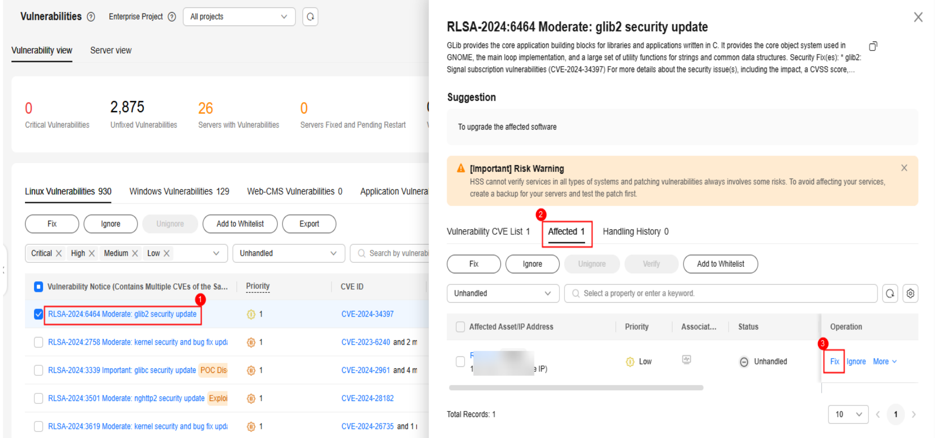
0 Critical Vulnerabilities | 3,361 Unfixed Vulnerabilities | 35 Servers with Vulnerabilities | 0 Servers Fixed and Pending Restart | 27/1,287 Vulnerabilities Handled Today/Total | 294,673 Detectable Vulnerabilities | 2,264 Total Scans, Last scanned:Mar 12, 2025 15:29:07

□ Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
□ CESA-2016:2587 Moderate CentOS 7 wget Security Update	2	CVE-2016-4971	8.8	Mar 12, 2025 17:07:45...	The wget packages provide the GNU Wget file retriev...	Fix Ignore Add to Wh
□ CESA-2017:3075 Important CentOS 7 wget Security Update	2	CVE-2017-13089 and 1 more	8.8	Mar 12, 2025 17:07:45...	The wget packages provide the GNU Wget file retriev...	Fix Ignore Add to Wh
□ CESA-2018:3221 Moderate CentOS 7 openssl Security Upda	2	CVE-2017-3735 and 4 more	7.5	Mar 12, 2025 17:07:45...	OpenSSL is a toolkit that implements the Secure Sock...	Fix Ignore Add to Wh

- Fix one or more servers affected by a vulnerability.
  1. Click a vulnerability name.
  2. On the vulnerability details slide-out panel displayed, click the **Affected** tab, locate the row containing the target server, and click **Fix** in the **Operation** column.

     You can also select all target servers and click **Fix** above the server list to fix vulnerabilities for the servers in batches.

Figure 5-17 Fix a server affected by a vulnerability



0 Critical Vulnerabilities | 2,875 Unfixed Vulnerabilities | 26 Servers with Vulnerabilities | 0 Servers Fixed and Pending Restart

☑ Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID
☑ RLSA-2024:6464 Moderate: glib2 security update	1	CVE-2024-34397
□ RLSA-2024:2758 Moderate: kernel security and bug fix upd:	1	CVE-2023-6240 and 2 m
□ RLSA-2024:3339 Important: glibc security update POC Dis	1	CVE-2024-2961 and 4 m
□ RLSA-2024:3501 Moderate: nghttp2 security update Exploi	1	CVE-2024-28182
□ RLSA-2024:3619 Moderate: kernel security and bug fix upd:	1	CVE-2024-26735 and 1

RLSA-2024:6464 Moderate: glib2 security update

GLib provides the core application building blocks for libraries and applications written in C. It provides the core object system used in GNOME, the main loop implementation, and a large set of utility functions for strings and common data structures. Security Fix(es): * glib2: Signal subscription vulnerabilities (CVE-2024-34397) For more details about the security issue(s), including the impact, a CVSS score,...

Suggestion

To upgrade the affected software

[Important] Risk Warning
HSS cannot verify services in all types of systems and patching vulnerabilities always involves some risks. To avoid affecting your services, create a backup for your servers and test the patch first.

□ Affected Asset/IP Address	Priority	Associat...	Status	Operation
□ [redacted] IP)	Low		Unhandled	Fix Ignore More

Total Records: 1

Step 5 In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets.

For Linux vulnerabilities, you can click **View details** in the **Fix** dialog box to view the name of the component to be fixed.

Step 6 (Optional) Back up servers.

Before fixing vulnerabilities, use HSS to back up servers, so that you can restore their data if it is affected by the fix. If you do not need to back up data, skip this step.

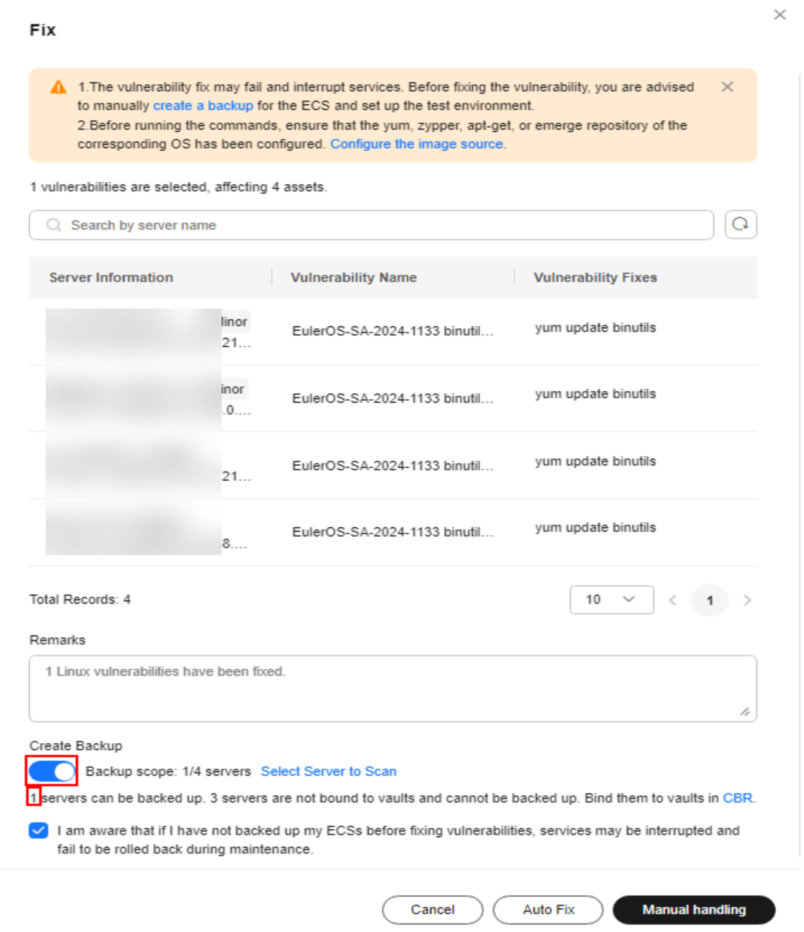
1. In the **Fix** dialog box, click to enable backup.

   NOTE

   – After backup is enabled, the number of servers that can be backed up will be displayed below the toggle switch. Only the servers associated with backup vaults can be backed up. For more information, see **Associating a Resource with the Vault**.

   – If backup is enabled in a vulnerability fix task, vulnerabilities can be fixed only on the servers that can be backed up in this task. For servers that fail to be backed up, start another vulnerability fix task for them.

Figure 5-18 Creating a backup



Fix

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

1 vulnerabilities are selected, affecting 4 assets.

Search by server name

Server Information	Vulnerability Name	Vulnerability Fixes
[redacted] linor 21...	EulerOS-SA-2024-1133 binutil...	yum update binutils
[redacted] inor .0....	EulerOS-SA-2024-1133 binutil...	yum update binutils
[redacted] 21...	EulerOS-SA-2024-1133 binutil...	yum update binutils
[redacted] 8....	EulerOS-SA-2024-1133 binutil...	yum update binutils

Total Records: 4 10 < 1 >

Remarks

1 Linux vulnerabilities have been fixed.

Create Backup

Backup scope: 1/4 servers Select Server to Scan

1 servers can be backed up. 3 servers are not bound to vaults and cannot be backed up. Bind them to vaults in CBR.

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

2. Choose **Select Server to Scan**. The backup creation dialog box is displayed.
3. In the **Create Backup** dialog box, set a backup file name, and click **OK**.

Step 7 In the **Fix** dialog box displayed, select **I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.** and click **Auto Fix**.

If you have manually fixed the vulnerability, click **Manual handling** in the **Fix** dialog box. After the vulnerability is manually handled, its status changes to **Fixed**. If the vulnerability is not successfully fixed, it will still be displayed in the vulnerability list after the next vulnerability scan completes.

Step 8 Click a vulnerability name.

Step 9 Click the **Handling History** tab to view the fix status of the target vulnerability in the **Status** column. **Table 5-7** describes vulnerability fix statuses.

NOTE

Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

Table 5-7 Vulnerability fix statuses

Status	Description
Unhandled	The vulnerability is not fixed.
Ignored	The vulnerability does not affect your services. You have ignored the vulnerability.
Verifying	HSS is verifying whether a fixed vulnerability is successfully fixed.
Fixing	HSS is fixing the vulnerability.
Fixed	The vulnerability has been successfully fixed.
Restart required	The vulnerability has been successfully fixed. You need to restart the server as soon as possible.
Failed	The vulnerability fails to be fixed. The possible cause is that the vulnerability does not exist or has been changed.
Restart the server and try again	This status is displayed only for vulnerabilities that exist on Windows servers. The vulnerability has not been fixed on the Windows server for a long time. As a result, the latest patch cannot be installed. You need to install an earlier patch, restart the server, and then install the latest patch.

----End

Automatically Fixing Vulnerabilities (Server View)

You can only fix Linux and Windows vulnerabilities with one-click on the console.

Step 1 Log in to the management console.

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

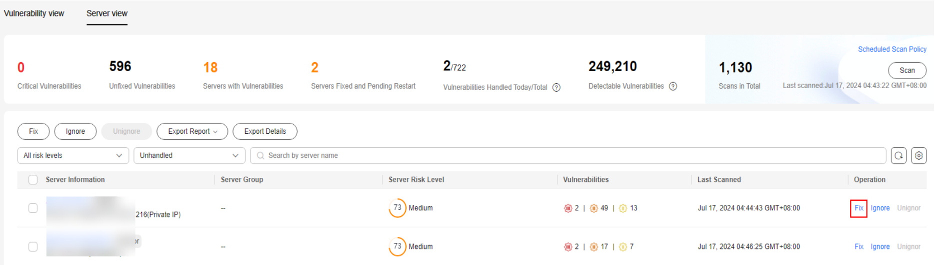
Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 Fix Linux and Windows vulnerabilities.

- Fixing all Linux or Windows vulnerabilities on a server
  a. Locate the row containing a target server and click **Fix** in the **Operation** column.

     You can also select multiple servers and click **Fix** in the upper part of the vulnerability list. To fix all server vulnerabilities, you just need to click **Fix** with no need of selecting servers.

     Figure 5-19 Fixing all the Linux or Windows vulnerabilities on a server



0 Critical Vulnerabilities
596 Unfixed Vulnerabilities
18 Servers with Vulnerabilities
2 Servers Fixed and Pending Restart
2/722 Vulnerabilities Handled Today/Total
249,210 Detectable Vulnerabilities
1,130 Scans in Total
Scheduled Scan Policy
Scan
Last scanned:Jul 17, 2024 04:43:22 GMT+08:00

☐ Server Information	Server Group	Server Risk Level	Vulnerabilities	Last Scanned	Operation
☐ [redacted] 216(Private IP)	--	73 Medium	2 | 49 | 13	Jul 17, 2024 04:44:43 GMT+08:00	Fix Ignore Unignor
☐ [redacted]	--	73 Medium	2 | 17 | 7	Jul 17, 2024 04:46:25 GMT+08:00	Fix Ignore Unignor

  b. In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets.

     For Linux vulnerabilities, you can view fix commands in the dialog box to view the name of the component to be fixed.

  c. (Optional) Back up servers.

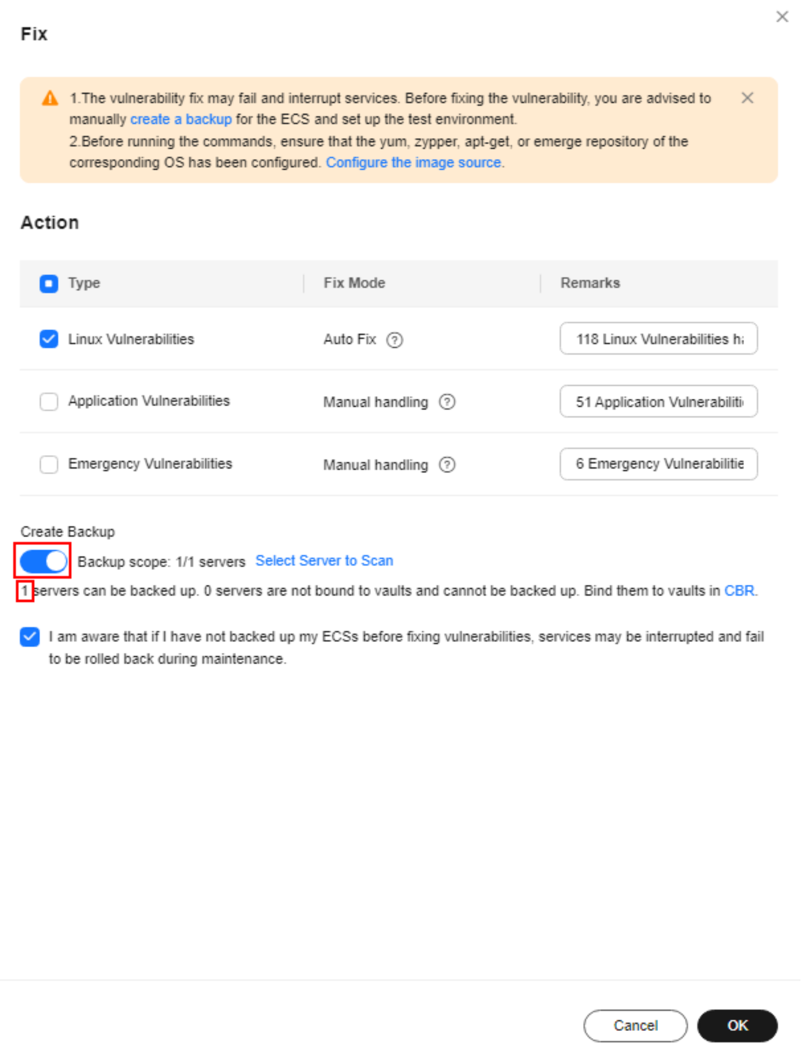
     Before fixing vulnerabilities, use HSS to back up servers, so that you can restore their data if it is affected by the fix. If you do not need to back up data, skip this step.

     i. In the **Fix** dialog box, click ○ to enable backup.

        NOTE

        - After backup is enabled, the number of servers that can be backed up will be displayed below the toggle switch. Only the servers associated with backup vaults can be backed up. For more information, see **Associating a Resource with the Vault**.
        - If backup is enabled in a vulnerability fix task, vulnerabilities can be fixed only on the servers that can be backed up in this task. For servers that fail to be backed up, start another vulnerability fix task for them.

Figure 5-20 Creating a configuration backup



Fix

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

Action

■ Type	Fix Mode	Remarks
☑ Linux Vulnerabilities	Auto Fix ⓘ	118 Linux Vulnerabilities h
□ Application Vulnerabilities	Manual handling ⓘ	51 Application Vulnerabiliti
□ Emergency Vulnerabilities	Manual handling ⓘ	6 Emergency Vulnerabilitie

Create Backup

Backup scope: 1/1 servers Select Server to Scan

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

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

ii. Choose **Select Server to Scan**. The backup creation dialog box is displayed.

iii. In the **Create Backup** dialog box, set a backup file name, and click **OK**.

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

Only Linux and Windows vulnerabilities can be automatically fixed with one-click. Web-CMS and application vulnerabilities need to be manually fixed by logging in to the server.

e. Click the server name. On the server details slide-out panel displayed, view the vulnerability fix status. Table 5-8 describes vulnerability fix statuses.

NOTE

Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

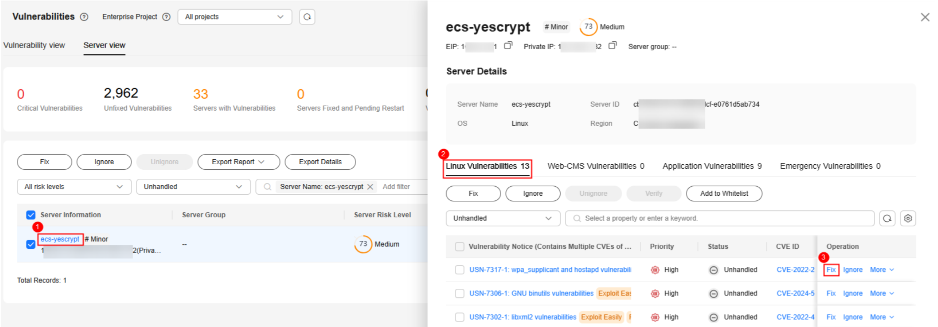
- Fixing one or more vulnerabilities on a server

  a. Click the name of a target server. The server details slide-out panel is displayed.

  b. Locate the row containing a target vulnerability and click **Fix** in the **Operation** column.

     Alternatively, you can select all target vulnerabilities and click **Fix** above the vulnerability list to fix vulnerabilities in batches. To fix all vulnerabilities, click **Fix** with no need of selecting any servers.

     Figure 5-21 Fixing a vulnerability on a server



  c. In the displayed dialog box, confirm the number of vulnerabilities to be fixed and the number of affected assets.

     For Linux vulnerabilities, you can view fix commands in the dialog box to view the name of the component to be fixed.

  d. (Optional) Back up servers.

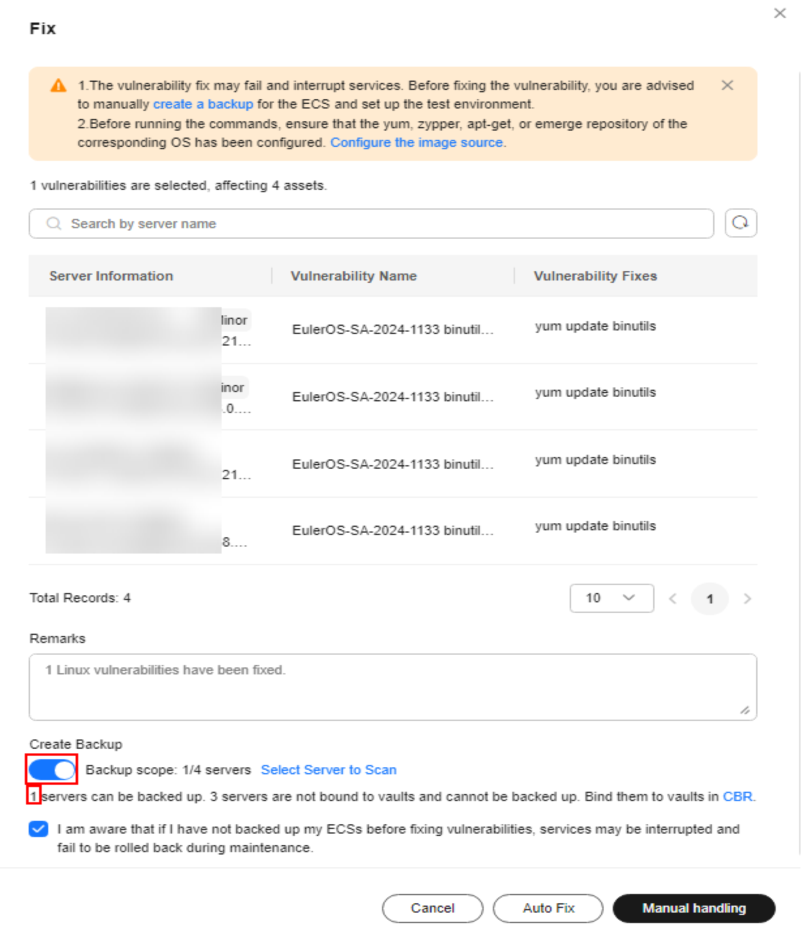
     Before fixing vulnerabilities, you can use HSS to back up servers, so that you can restore their data if it is affected by the fix. If you do not need to back up data, skip this step.

     i. In the **Fix** dialog box, click ◯ to enable backup.

        NOTE

        - After backup is enabled, the number of servers that can be backed up will be displayed below the toggle switch. Only the servers associated with backup vaults can be backed up. For more information, see **Associating a Resource with the Vault**.
        - If backup is enabled in a vulnerability fix task, vulnerabilities can be fixed only on the servers that can be backed up in this task. For servers that fail to be backed up, start another vulnerability fix task for them.

Figure 5-22 Creating a backup



Fix

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

1 vulnerabilities are selected, affecting 4 assets.

Search by server name

Server Information	Vulnerability Name	Vulnerability Fixes
[redacted]	EulerOS-SA-2024-1133 binutil...	yum update binutils
[redacted]	EulerOS-SA-2024-1133 binutil...	yum update binutils
[redacted]	EulerOS-SA-2024-1133 binutil...	yum update binutils
[redacted]	EulerOS-SA-2024-1133 binutil...	yum update binutils

Total Records: 4

Remarks

1 Linux vulnerabilities have been fixed.

Create Backup

Backup scope: 1/4 servers Select Server to Scan

1 servers can be backed up. 3 servers are not bound to vaults and cannot be backed up. Bind them to vaults in CBR.

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

ii. Choose **Select Server to Scan**. The backup creation dialog box is displayed.

iii. In the **Create Backup** dialog box, set a backup file name, and click **OK**.

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

If you have manually fixed the vulnerability, click **Manual handling** in the **Fix** dialog box. After the vulnerability is manually handled, its status changes to **Fixed**. If the vulnerability is not successfully fixed, it will still be displayed in the vulnerability list after the next vulnerability scan completes.

f. In the **Status** column of the target vulnerability, view the fix status of the vulnerability. **Table 5-8** describes vulnerability fix statuses.

NOTE

Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.

Table 5-8 Vulnerability fix statuses

Status	Description
Unhandled	The vulnerability is not fixed.
Ignored	The vulnerability does not affect your services. You have ignored the vulnerability.
Verifying	HSS is verifying whether a fixed vulnerability is successfully fixed.
Fixing	HSS is fixing the vulnerability.
Fixed	The vulnerability has been successfully fixed.
Restart required	The vulnerability has been successfully fixed. You need to restart the server as soon as possible.
Failed	The vulnerability fails to be fixed. The possible cause is that the vulnerability does not exist or has been changed.
Restart the server and try again	This status is displayed only for vulnerabilities that exist on Windows servers. The vulnerability has not been fixed on the Windows server for a long time. As a result, the latest patch cannot be installed. You need to install an earlier patch, restart the server, and then install the latest patch.

----End

Manually Fixing Vulnerabilities

HSS cannot automatically fix Web-CMS vulnerabilities, application vulnerabilities, and emergency vulnerabilities in one click. You can log in to the server to manually fix them by referring to the fix suggestions on the vulnerability details slide-out panel.

NOTE

- Restart the system after you fixed a Windows OS or Linux kernel vulnerability, or HSS will probably continue to warn you of this vulnerability.
- Fix the vulnerabilities in sequence based on the suggestions.
- If multiple software packages on the same server have the same vulnerability, you only need to fix the vulnerability once.

Viewing vulnerability fix suggestions

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 Click the name of a target vulnerability to access the vulnerability details slide-out panel and view the fix suggestions.

----End

Fixing vulnerabilities by referring to vulnerability fix suggestions

Vulnerability fix may affect service stability. You are advised to use either of the following methods to avoid such impact:

- Method 1: Create a new VM to fix the vulnerability.

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

  a. Create an image for the ECS to be fixed. For details, see **Creating a Full-ECS Image Using an ECS**.

  b. Use the image to create an ECS. For details, see **Creating ECSs Using an Image**.

  c. Fix the vulnerability on the new ECS and verify the result.

  d. Switch services over to the new ECS and verify they are stably running.

  e. Release the original ECS. If a fault occurs after the service switchover and cannot be rectified, you can switch services back to the original ECS.

- Method 2: Fix the vulnerability on the target server.

  Use this method if you have fixed the vulnerability on similar servers before.

  a. Create a backup for the ECS whose vulnerabilities need to be fixed. For details, see **Creating a CSBS Backup**.

  b. Fix vulnerabilities on the current server.

  c. If services become unavailable after the vulnerability is fixed and cannot be recovered in a timely manner, use the backup to restore the server. For details, see **Using Backups to Restore Servers**.

NOTE

After the vulnerability is manually fixed, you are advised to **verify the vulnerability fix**.

Ignoring a Vulnerability

Some vulnerabilities are risky only in specific conditions. For example, if a vulnerability can be exploited only through an open port, but the target server does not open any ports, the vulnerability will not harm the server. Such vulnerabilities can be ignored. HSS will not generate alarms for ignored vulnerabilities.

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

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

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 Locate the row containing a target vulnerability and click **Ignore** in the **Operation** column.

Step 5 In the dialog box displayed, click **OK**.

----End

Adding a Vulnerability Whitelist Item

If you evaluate that some vulnerabilities do not affect your services and do not want to view the vulnerabilities in the vulnerability list, you can whitelist the vulnerabilities. After they are whitelisted, the vulnerabilities will be ignored in the vulnerability list and no alarms will be reported. The vulnerabilities will not be scanned and the vulnerability information will not be displayed when the next vulnerability scan task is executed.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

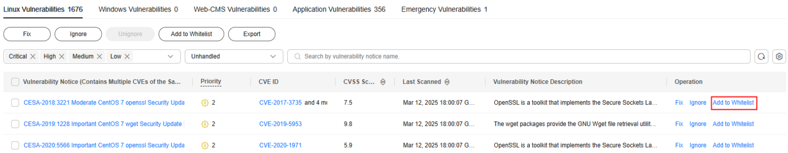
- Whitelisting all servers that are affected by a vulnerability

  HSS will ignore the vulnerability when scanning for vulnerabilities on all servers.

  a. In the **Operation** column of a vulnerability, click **Add to Whitelist**.

     You can also select multiple vulnerabilities and click **Add to Whitelist** above the vulnerability list.

     Figure 5-23 Whitelisting all servers that are affected by a vulnerability

     
Linux Vulnerabilities 1676
Windows Vulnerabilities 0
Web-CMS Vulnerabilities 0
Application Vulnerabilities 356
Emergency Vulnerabilities 1
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical × High × Medium × Low ×
Unhandled
Search by vulnerability notice name.

□ Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID	CVSS Sc...	Last Scanned	Vulnerability Notice Description	Operation
□ CESA-2018:3221 Moderate CentOS 7 openssl Security Upda	2	CVE-2017-3735 and 4 mo	7.5	Mar 12, 2025 18:00:07 G...	OpenSSL is a toolkit that implements the Secure Sockets La...	Fix Ignore Add to Whitelist
□ CESA-2019:1228 Important CentOS 7 wget Security Update	2	CVE-2019-5953	9.8	Mar 12, 2025 18:00:07 G...	The wget packages provide the GNU Wget file retrieval utilit...	Fix Ignore Add to Whitelist
□ CESA-2020:5566 Important CentOS 7 openssl Security Upda	2	CVE-2020-1971	5.9	Mar 12, 2025 18:00:07 G...	OpenSSL is a toolkit that implements the Secure Sockets La...	Fix Ignore Add to Whitelist

  b. In the dialog box displayed, click **OK**.

- Whitelisting one or more servers that are affected by a vulnerability

  HSS will ignore the vulnerability when scanning for vulnerabilities on these servers.

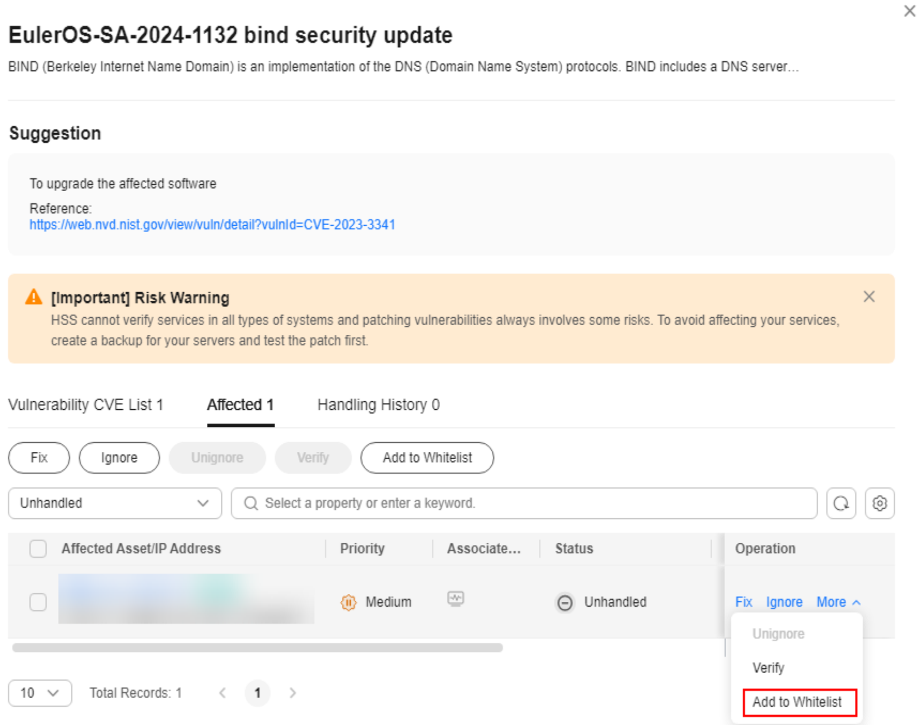
  a. Click a target vulnerability name.

  b. On the slide-out panel displayed, click the **Affected** tab.

  c. In the **Operation** column of the row containing the target server, click **More** and select **Add to Whitelist**.

     You can also select multiple servers and click **Add to Whitelist** above the server list.

Figure 5-24 Whitelisting a single server that is affected by a vulnerability



EulerOS-SA-2024-1132 bind security update

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server...

Suggestion

To upgrade the affected software

Reference:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-3341

[Important] Risk Warning
HSS cannot verify services in all types of systems and patching vulnerabilities always involves some risks. To avoid affecting your services, create a backup for your servers and test the patch first.

□	Affected Asset/IP Address	Priority	Associate...	Status	Operation
□	[redacted]	Medium		Unhandled	Fix Ignore More

d. In the dialog box displayed, click **OK**.

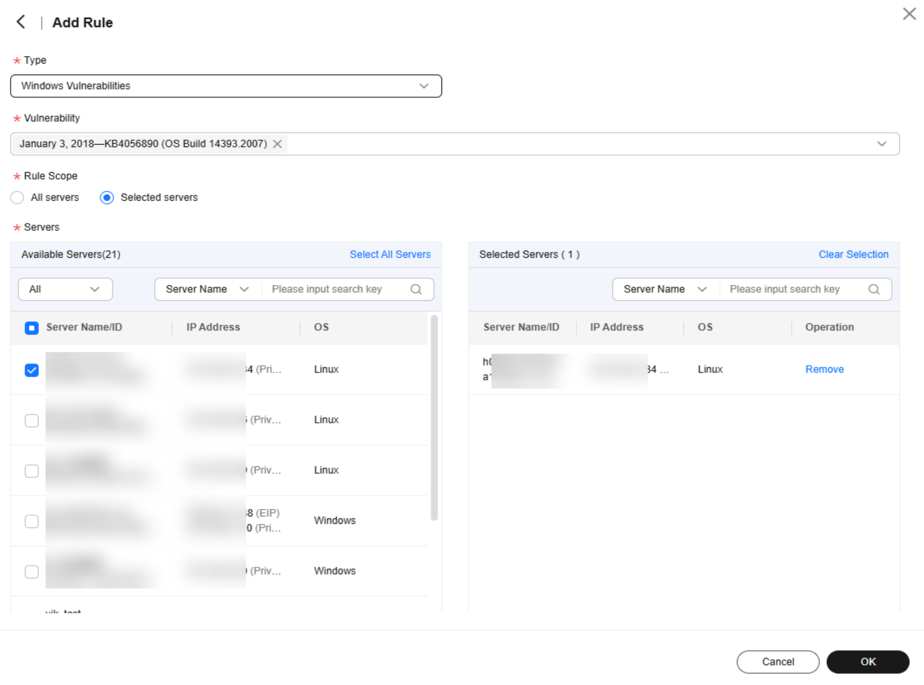
- Whitelisting vulnerabilities using whitelist rules

a. In the upper right corner of the **Vulnerabilities** page, click **Vulnerability Whitelist**.

b. In the **Vulnerability Whitelist** area, click **Add Rule**.

c. Configure a whitelist rule according to **Table 5-9**.

Figure 5-25 Configuring a whitelist rule



Add Rule

* Type: Windows Vulnerabilities

* Vulnerability: January 3, 2018—KB4056890 (OS Build 14393.2007)

* Rule Scope: ○ All servers ● Selected servers

* Servers

☑	Server Name/ID	IP Address	OS
☑	[redacted]	[redacted]4 (Pri...	Linux
□	[redacted]	[redacted] (Priv...	Linux
□	[redacted]	[redacted] (Priv...	Linux
□	[redacted]	[redacted]8 (EIP) [redacted]0 (Pri...	Windows
□	[redacted]	[redacted] (Priv...	Windows

Server Name/ID	IP Address	OS	Operation
[redacted]	[redacted]34 ...	Linux	Remove

Table 5-9 Vulnerability whitelist rule parameters

Parameter	Description
Type	Select the type of vulnerabilities to be whitelisted. Possible values are as follows: ▪ **Linux Vulnerabilities** ▪ **Windows Vulnerabilities** ▪ **Web-CMS Vulnerabilities** ▪ **Application Vulnerabilities** ▪ **Emergency Vulnerabilities**
Vulnerability	Select one or more vulnerabilities to be whitelisted.
Rule Scope	Select the servers affected by the vulnerabilities. Possible values are as follows: ▪ **All servers** HSS will ignore the vulnerability when scanning for vulnerabilities on all servers. ▪ **Selected servers** Select one or more target servers. HSS will ignore the vulnerabilities when scanning for vulnerabilities on these servers. You can search for a target server by server name, ID, EIP, or private IP address.
Remarks (Optional)	Enter the remarks.

d. Click **OK**.

----End

Verifying the Vulnerability Fix

After you manually fix vulnerabilities, you are advised to verify the fixing result.

- **Method 1**: On the vulnerability details page, click **More** > **Verify** to perform one-click verification. This method has the following restrictions:
  - The fix of emergency vulnerabilities cannot be verified.
  - Only the fix of the application vulnerabilities of the JAR package can be verified. The application vulnerabilities of non-JAR packages are automatically filtered out and not verified.
- **Method 2**: Ensure the software has been upgraded to the latest version. The following table provides the commands to check the software upgrade result.

Table 5-10 Verification commands

OS	Command
CentOS/Fedora /Euler/Red Hat/Oracle	rpm -qa | grep *Software_name*
Debian/Ubuntu	dpkg -l | grep *Software_name*
Gentoo	emerge --search *Software_name*

- **Method 3**: **Manually check for vulnerabilities** and view the vulnerability fixing results.

FAQ

What Do I Do If Vulnerability Fix Failed?

5.1.6 Managing the Vulnerability Whitelist

If you evaluate that some vulnerabilities do not affect your services and do not want to view the vulnerabilities in the vulnerability list, you can whitelist the vulnerabilities. After they are whitelisted, the vulnerabilities will be ignored in the vulnerability list and no alarms will be reported. The vulnerabilities will not be scanned and the vulnerability information will not be displayed when the next vulnerability scan task is executed.

This section describes how to modify and remove an item in the vulnerability whitelist.

Constraints

The basic edition does not support this function. For details about how to buy and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.

Editing a Vulnerability Whitelist

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

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

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 In the upper right corner of the **Vulnerabilities** page, click **Vulnerability Whitelist**.

Step 5 In the row containing the desired vulnerability whitelist rule, click **Edit** in the **Operation** column.

Step 6 On the editing page, modify the information and click **OK**.

----End

Removing a Vulnerability Whitelist Rule from the Vulnerability Whitelist

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 In the upper right corner of the **Vulnerabilities** page, click **Vulnerability Whitelist**.

Step 5 In the row containing the desired vulnerability whitelist rule, click **Delete** in the **Operation** column.

Step 6 In the dialog box displayed, confirm the information and click **OK**.

----End

5.1.7 Viewing Vulnerability Handling History

For vulnerabilities that have been handled, you can refer to this section to view the vulnerability handling history (handler and handling time).

Constraints

- The basic edition does not support this function. For details about how to buy and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.
- Handling history can be retained for a maximum of 180 days.

Viewing the Handling History of a Vulnerability

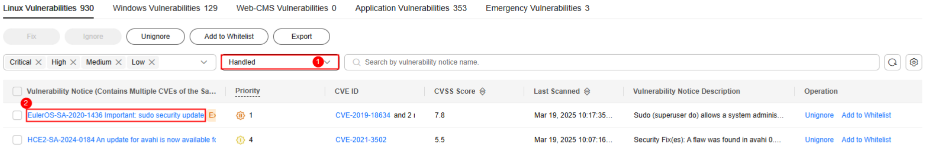
Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Risk Management** > **Vulnerabilities**.

Step 4 In the list of handled vulnerabilities, click a vulnerability name. The vulnerability details slide-out panel is displayed.

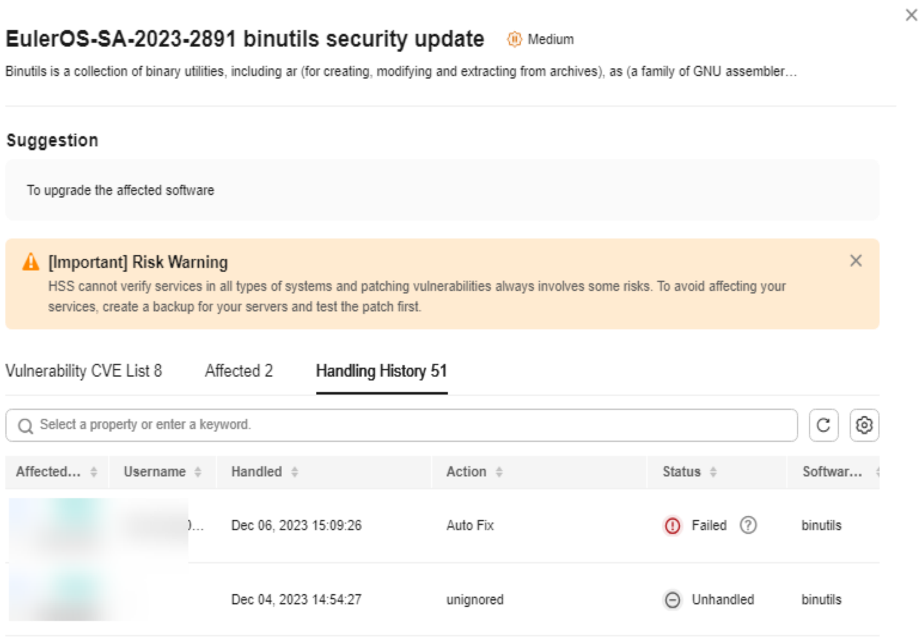
Figure 5-26 Selecting Handled from the drop-down list


Linux Vulnerabilities 930
Windows Vulnerabilities 129
Web-CMS Vulnerabilities 0
Application Vulnerabilities 353
Emergency Vulnerabilities 3
Fix
Ignore
Unignore
Add to Whitelist
Export
Critical ✕ High ✕ Medium ✕ Low ✕
Handled
1
Search by vulnerability notice name.
2

Vulnerability Notice (Contains Multiple CVEs of the Sa...	Priority	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
EulerOS-SA-2020-1436 Important: sudo security update	1	CVE-2019-18634 and 2	7.8	Mar 19, 2025 10:17:35...	Sudo (superuser do) allows a system adminis...	Unignore Add to Whitelist
HCE2-SA-2024-0184 An update for avahi is now available fo	4	CVE-2021-3502	5.5	Mar 19, 2025 10:07:16...	Security Fix(es): A flaw was found in avahi 0....	Unignore Add to Whitelist

Step 5 Click the **Handling History** tab to view the handling history of the vulnerability.

Figure 5-27 Handling history



EulerOS-SA-2023-2891 binutils security update Medium

Binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assembler...

Suggestion

To upgrade the affected software

[Important] Risk Warning

HSS cannot verify services in all types of systems and patching vulnerabilities always involves some risks. To avoid affecting your services, create a backup for your servers and test the patch first.

Affected...	Username	Handled	Action	Status	Softwar...
[redacted]	[redacted]	Dec 06, 2023 15:09:26	Auto Fix	Failed	binutils
[redacted]		Dec 04, 2023 14:54:27	unignored	Unhandled	binutils

----End

Viewing the Handling History of All Vulnerabilities

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Security Operations** > **Handling History**. The **Handling History** page is displayed.

Step 4 On the **Vulnerabilities** tab page displayed, view the handling history of all vulnerabilities.

- Viewing the vulnerability handling history of a specified enterprise project

  In the upper left corner of the **Handling History** page, select an enterprise project for **Enterprise Project** to view the handling history of server vulnerabilities in the enterprise project.

- Viewing the vulnerability handling history of a specified property

  In the search box above the vulnerability handling history list, select an attribute or enter a keyword to search for the handling records of a specified attribute.

----End

5.2 Baseline Check

5.2.1 Baseline Check Overview

What Is a Baseline Check?

Baselines specify the recommended security configurations for OSs, databases, middleware, and applications. They include the configurations of permissions, services, network, password security, and DJCP MLPS compliance.

HSS can check password complexity policies, common weak passwords, and other settings to detect insecure passwords and the configuration risks in systems and critical software. It also provides suggestions to help users correctly handle unsafe settings on servers.

Baseline Check Content

Check Item	Description	Supported HSS Edition
Baseline check	Check the unsafe Tomcat, Nginx, SSH login, and system configurations found by HSS. The configuration check standards include cloud security practices, DJCP MLPS compliance, and the general security standard. ● Cloud security practices: Based on Huawei Cloud's years of experience in cloud security practices, the service checks the security of systems and software in terms of account management, authentication and authorization, password policies, log management, service management, network configuration, and patch update. ● DJCP MLPS compliance: Check the security of systems and databases based on the DJCP Multi-Level Protection Scheme (MLPS) standard and the evaluation standards of authoritative organizations. ● General security standard: Based on China and international general security standards, check the security of the system and software from the perspectives of account management, password policy, authorization management, service management, configuration management, network management, and permission management. The following systems, databases, and applications can be checked: ● For Linux, – Cloud security practices: Apache HTTP Server 2.4, Apache 2, ClickHouse 21.8, CentOS 7, Docker, Docker 18, EulerOS, Gauss, HCE 1.1, HCE 2.0, Kafka, MongoDB, MySQL 5.7, MySQL 5, Nginx, Nginx 1.17, openGauss, Redis, Redis 5.0, Redis 6.2, SSH, Tomcat, Tomcat 8, Tomcat 9, Zookeeper 3.6, Zookeeper 3.7, Kubernetes-Master, and Kubernetes-Node. – DJCP MLPS compliance: Apache 2, MongoDB, MySQL 5, Nginx, Tomcat, CentOS 7, CentOS 8, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu12, Ubuntu14, Ubuntu16, Ubuntu18, SUSE 12, SUSE 15, HCE1.1, EulerOS, and Alma. – General security standards: MySQL8-universal, HCE1.1-universal, Rocky8-universal, Rocky9-	Enterprise, premium, WTP, and container editions

Check Item	Description	Supported HSS Edition
	universal, AlmaLinux8-universal, OracleLinux6-universal, OracleLinux7-universal, Ubuntu22-universal, Ubuntu24-universal, Ubuntu20-universal, CentOS7-universal, CentOS8-universal, CentOS9-universal, SUSE15-universal, AliLinux2-universal, and AliLinux3-universal. **NOTE** The MySQL baseline detection of Linux OS is based on the MySQL 5 security configuration specifications. If MySQL 8 is installed on your server, the following check items are not displayed in the detection results, because they are discarded in that version. The detection results are displayed only on the server whose MySQL version is 5. ● Rule: Do not set **old_passwords** to **1**. ● Rule: Set secure_auth to **1** or **ON**. ● Rule: Do not set **skip_secure_auth**. ● Rule: Set **log_warnings** to **2**. ● Rule: Configure the MySQL binlog clearing policy. ● Rule: The **sql_mode** parameter contains **NO_AUTO_CREATE_USER**. ● Rule: Use the MySQL audit plug-in. ● For Windows, – Cloud security practices: Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 R2, Windows Server 2019 R2, Tomcat, Redis, Nginx, MySQL 5, MongoDB, and Apache 2 – General security standard: Windows Server 2022 R2.	

Check Item	Description	Supported HSS Edition
Password complexity policies	A password complexity policy specifies the rules that must be followed by user passwords to improve password security and prevent brute-force attacks. This feature checks the password complexity policies in Linux and provides suggestions to help users improve password security. Check items include: ● Password length: Check whether the password length required in the password complexity policy meets the security standard. ● Uppercase letters: Check whether the number of uppercase letters required in the password complexity policy meets the security standard. ● Lowercase letters: Check whether the number of lowercase letters required in the password complexity policy meets the security standard. ● Numeric characters: Check whether the number of numeric characters required in the password complexity policy meets the security standard. ● Special letters: Check whether the number of special characters required in the password complexity policy meets the security standard. For details about the password complexity policy check, see **Defining a Rule to Check Password Complexity Policies**.	All
Common weak passwords	A weak password can be easily cracked. Weak passwords defined in the common weak password library. You can check for the weak passwords used by accounts and remind users to change them. Common weak password detection has the following restrictions: ● Supported cryptographic algorithms: SHA-256, SHA-512, and Yescrypt ● Supported account types: – Linux: MySQL, FTP, Redis, and system accounts – Windows: system accounts For details about custom weak passwords, see **Defining Weak Passwords**.	All

Scenarios

- Baseline compliance

  Baseline checks are performed based on DJCP MLPS L2, DJCP MLPS L3, and international compliance security standards, helping companies build information systems that comply with related laws and regulations as well as industry standards.
- Security audit

  Periodically perform baseline checks on servers and containers to detect and rectify non-compliant system configurations in a timely manner, ensuring system security and reducing intrusion risks.

Usage Process

Table 5-11 Usage process

No.	Operation	Description
1	**Configuring a Baseline Check Policy**	After HSS is enabled for a server, HSS automatically performs a baseline check on the server every day from 04:00 to 05:00 based on the default policy. If the default configuration does not meet your requirements, you can modify it or create a custom check policy.
2	**Performing a Baseline Check**	You can perform a check immediately or schedule it for later. ● Scheduled check: Baseline checks are automatically performed based on the default policy or your schedule. ● One-time manual check: You can manually start a baseline check to learn the server security status in real time.
3	**Viewing and Handling Baseline Check Results**	After the baseline check is complete, view and handle the baseline configuration risks in a timely manner.

5.2.2 Configuring a Baseline Check Policy

Scenarios

Two scheduled check policies, **Advanced policy** and **Basic policy**, have been preconfigured in HSS. If HSS is enabled for a server, the server will be bound to either of these policies by default. HSS will automatically perform a baseline check some time between 04:00 to 05:00 every day.

- **Advanced policy**

When you enable the HSS enterprise, premium, container, or WTP edition for a server, the advanced policy will be bound to the server by default. The check items of the policy vary depending on the OS type (Windows or Linux):

- Linux: Baseline settings, password complexity policies, and common weak passwords
- Windows: Baseline settings and common weak passwords

For details about how to modify the check items, check time, and scanned servers of the advanced policy, see **Modifying an Advanced Policy**.

- **Basic policy**

  When you enable the HSS basic or professional edition for a server, the basic policy will be bound to the server by default. The check items of the policy vary depending on the OS type (Windows or Linux):

  - Linux: Common weak passwords and password complexity policies
  - Windows: Common weak passwords

  For details about how to modify the check items, check time, and scanned servers of the basic policy, see **Modifying a Basic Policy**.

You can create custom check policies in the HSS enterprise, premium, container, and WTP editions, for either one-time or periodic checks. If you do not want to bind the advanced policy to all servers, you can create custom policies for refined management. For details, see **Creating a Custom Check Policy**.

After configuring a default or custom policy, you can define the rules for checking password complexity policies and weak passwords. For details, see **Defining a Rule to Check Password Complexity Policies** and **Defining Weak Passwords**.

Constraints

- Each server can only be bound to a single scheduled scan policy (including the default one). When a server is bound to a new scheduled policy, it is automatically unbound from any existing policies.
- Each server can be bound to multiple one-time scan policies.

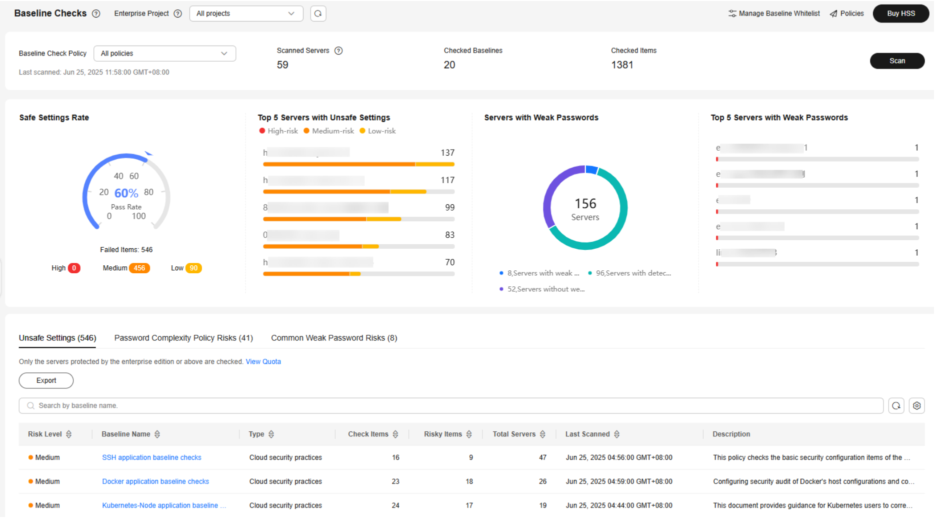
Modifying an Advanced Policy

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

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

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

Figure 5-28 Baseline checks



Baseline Checks
Enterprise Project
All projects
Manage Baseline Whitelist
Policies
Buy HSS
Scan
Safe Settings Rate
40 60
20 60% 80
Pass Rate
0 100
Top 5 Servers with Unsafe Settings
● High-risk ● Medium-risk ● Low-risk
137
117
99
83
70
Servers with Weak Passwords
156
Servers
● 8,Servers with weak ...
● 96,Servers with detec...
● 52,Servers without we...
Top 5 Servers with Weak Passwords
1
1
1
1
1
Unsafe Settings (546)
Password Complexity Policy Risks (41)
Common Weak Password Risks (8)
Export
Search by baseline name.

Baseline Check Policy: All policies

Last scanned: Jun 25, 2025 11:58:00 GMT+08:00

Scanned Servers: 59

Checked Baselines: 20

Checked Items: 1381

Failed Items: 546

High 0 Medium 456 Low 90

Only the servers protected by the enterprise edition or above are checked. View Quota

Risk Level	Baseline Name	Type	Check Items	Risky Items	Total Servers	Last Scanned	Description
● Medium	SSH application baseline checks	Cloud security practices	16	9	47	Jun 25, 2025 04:56:00 GMT+08:00	This policy checks the basic security configuration items of the ...
● Medium	Docker application baseline checks	Cloud security practices	23	18	26	Jun 25, 2025 04:59:00 GMT+08:00	Configuring security audit of Docker's host configurations and co...
● Medium	Kubernetes-Node application baseline ...	Cloud security practices	24	17	19	Jun 25, 2025 04:44:00 GMT+08:00	This document provides guidance for Kubernetes users to corre...

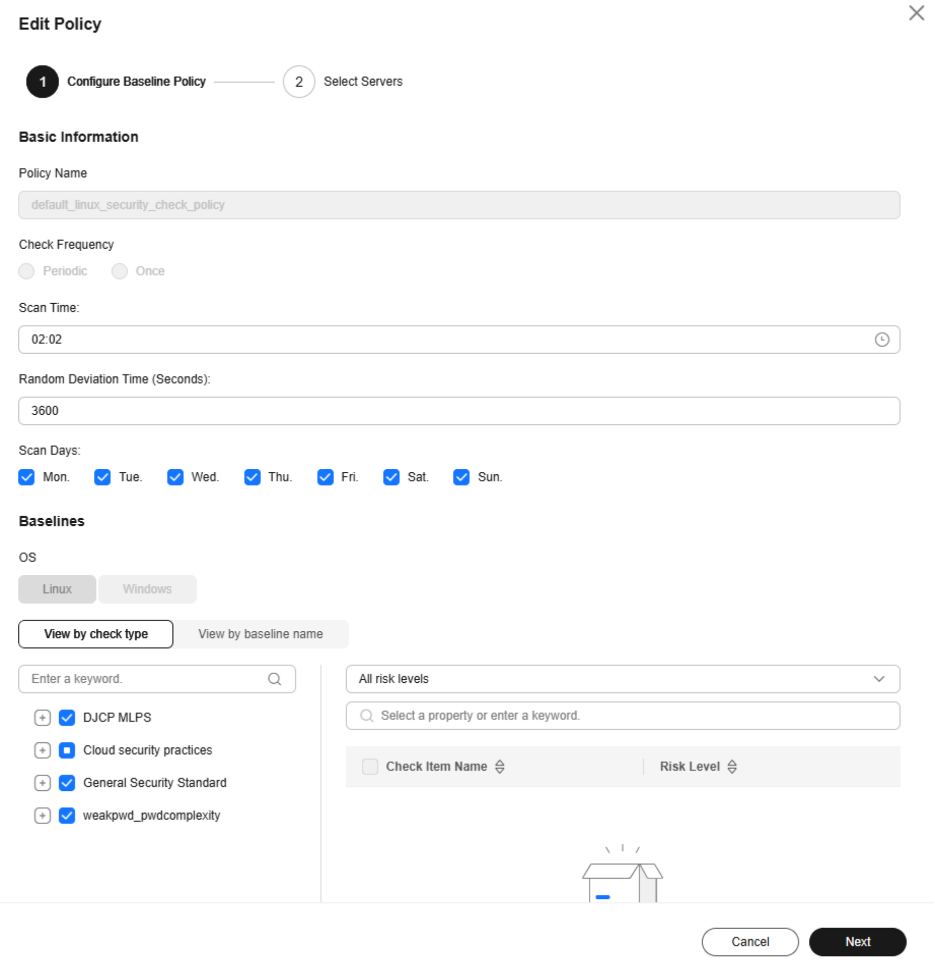
Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the upper right corner of the page, click **Policies**.

Step 6 In the **Operation** column of an **Advanced policy**, click **Edit**. Modify the policy on the edit page.

Step 7 Configure the baseline check policy as needed. For more information, see **Table 5-12**.

Figure 5-29 Editing an advanced policy



Edit Policy

1 Configure Baseline Policy — 2 Select Servers

Basic Information

Policy Name

default_linux_security_check_policy

Check Frequency

○ Periodic ○ Once

Scan Time:

02:02

Random Deviation Time (Seconds):

3600

Scan Days:

☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. ☑ Sat. ☑ Sun.

Baselines

OS

Linux Windows

View by check type | View by baseline name

Enter a keyword.

- ☑ DJCP MLPS
- ■ Cloud security practices
- ☑ General Security Standard
- ☑ weakpwd_pwdcomplexity

All risk levels

Select a property or enter a keyword.

□ Check Item Name	Risk Level

Table 5-12 Advanced policy parameters

Parameter	Description	Recommended Value
Policy Name	Default advanced policy name. It cannot be changed. ● Linux: **default_linux_security_check_policy** ● Windows: **default_windows_security_check_policy**	-
Check Frequency	The default value is **Periodic** and cannot be changed.	-
Scan Time	Click the input box and set the scan time.	04:00

Parameter	Description	Recommended Value
Random Deviation Time (Seconds)	Enter the allowed delay (in seconds) of a scan task. The value must be a positive integer. For example, if the scan time is 04:00 and the random deviation time is 3,600 seconds, the scan task will be performed sometime between 04:00 and 05:00.	3600
Scan Days	Select the days of a week for scans. The options include Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
Baselines	● **OS** The default value is used and cannot be changed. ● **Baseline** Select baselines. You can click **View by check type** or **View by baseline name** to browse faster. – You can select top-level types **DJCP MLPS Compliance**, **Cloud security practices**, **General Security Standard**, and **Weak Password & Password Complexity**. – You can click the ⊞ next to a top-level type to expand level-2 types. – You can click the ⊞ next to a level-2 type to expand level-3 types. – After you click a level-2 or level-3 type, the check items of that type will be displayed in the list on the right. – If you click **Common weak passwords** or **Password complexity check** (supported for Linux only), you can click **Define** in the area on the right to define the rules for checking common weak passwords or password complexity policies. You can also configure them on the **Baseline Checks** page. For details, see **Defining a Rule to Check Password Complexity Policies** and **Defining Weak Passwords**. For more information, see **Baseline Check Content**.	● **OS**: - ● **Baselines**: Select all.

Step 8 Confirm parameter settings and click **Next**.

Step 9 Select the servers where the policy is to be applied. Click **OK**.

----End

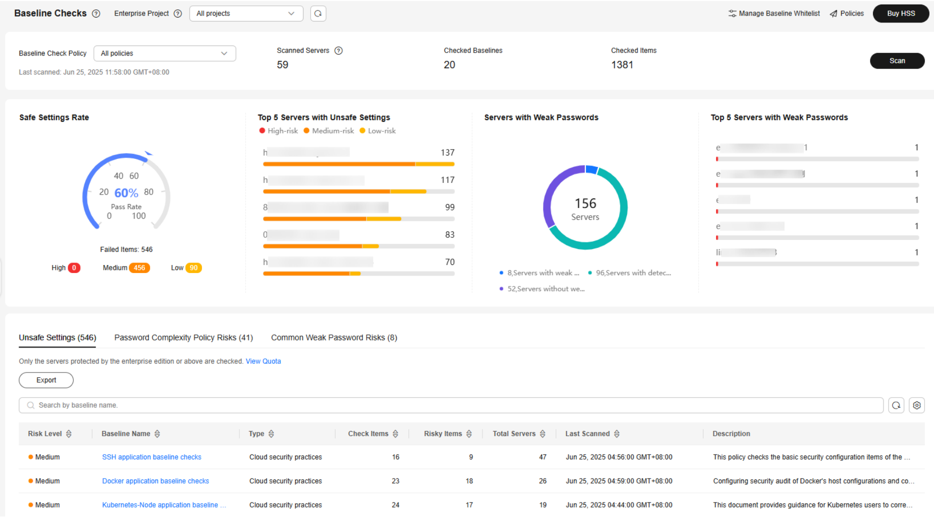
Modifying a Basic Policy

Step 1 Log in to the management console.

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

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

Figure 5-30 Baseline checks


Baseline Checks
Enterprise Project
Manage Baseline Whitelist
Policies
Buy HSS
Scan
Safe Settings Rate
40 60
20 60% 80
Pass Rate
0 100
Top 5 Servers with Unsafe Settings
● High-risk ● Medium-risk ● Low-risk
137
117
99
83
70
Servers with Weak Passwords
156
Servers
● 8,Servers with weak ...
● 96,Servers with detec...
● 52,Servers without we...
Top 5 Servers with Weak Passwords
1
1
1
1
1
Unsafe Settings (546)
Password Complexity Policy Risks (41)
Common Weak Password Risks (8)
Export
Search by baseline name.

Enterprise Project: All projects

Baseline Check Policy: All policies

Last scanned: Jun 25, 2025 11:58:00 GMT+08:00

Scanned Servers: 59

Checked Baselines: 20

Checked Items: 1381

Failed Items: 546

High 0 Medium 456 Low 90

Only the servers protected by the enterprise edition or above are checked. View Quota

Risk Level	Baseline Name	Type	Check Items	Risky Items	Total Servers	Last Scanned	Description
● Medium	SSH application baseline checks	Cloud security practices	16	9	47	Jun 25, 2025 04:56:00 GMT+08:00	This policy checks the basic security configuration items of the ...
● Medium	Docker application baseline checks	Cloud security practices	23	18	26	Jun 25, 2025 04:59:00 GMT+08:00	Configuring security audit of Docker's host configurations and co...
● Medium	Kubernetes-Node application baseline ...	Cloud security practices	24	17	19	Jun 25, 2025 04:44:00 GMT+08:00	This document provides guidance for Kubernetes users to corre...

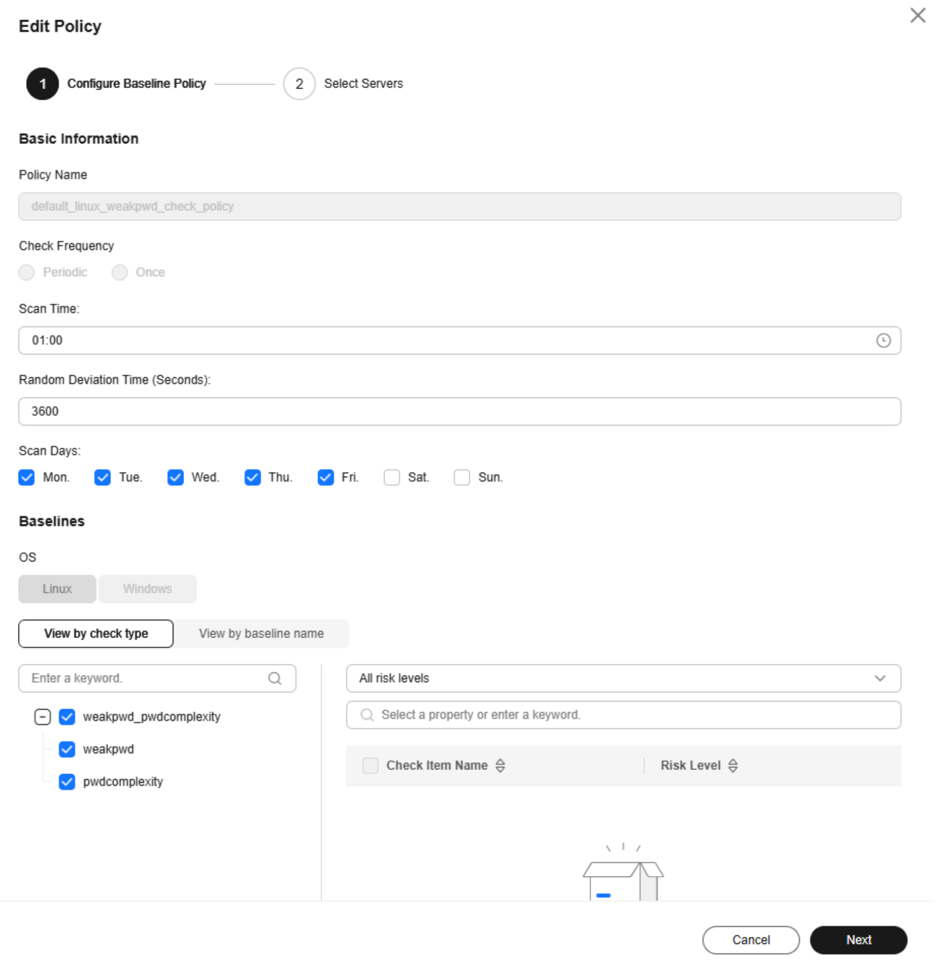
Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the upper right corner of the page, click **Policies**.

Step 6 In the **Operation** column of a **Basic policy**, click **Edit**. Modify the policy on the edit page.

Step 7 Configure the baseline check policy as needed. For more information, see **Table 5-13**.

Figure 5-31 Editing a basic policy



Edit Policy

1 Configure Baseline Policy — 2 Select Servers

Basic Information

Policy Name: default_linux_weakpwd_check_policy

Check Frequency: ○ Periodic ○ Once

Scan Time: 01:00

Random Deviation Time (Seconds): 3600

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

Baselines

OS: Linux | Windows

View by check type | View by baseline name

Enter a keyword.

- ☑ weakpwd_pwdcomplexity
  - ☑ weakpwd
  - ☑ pwdcomplexity

All risk levels

Select a property or enter a keyword.

□ Check Item Name	Risk Level

Table 5-13 Basic policy parameters

Parameter	Description	Recommended Value
Policy Name	Default basic policy name. It cannot be changed. ● Linux: **default_linux_weakpwd_check_policy** ● Windows: **default_windows_weakpwd_check_policy**	-
Check Frequency	The default value is **Periodic** and cannot be changed.	-
Scan Time	Click the input box and set the scan time.	04:00

Parameter	Description	Recommended Value
Random Deviation Time (Seconds)	Enter the allowed delay (in seconds) of a scan task. The value must be a positive integer. For example, if the scan time is 04:00 and the random deviation time is 3,600 seconds, the scan task will be performed sometime between 04:00 and 05:00.	3600
Scan Days	Select the days of a week for scans. The options include Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
Baselines	● **OS** The default value is used and cannot be changed. ● **Baseline** Select baseline check items. For Linux, you can select **Common weak passwords** or **Password complexity check**. For Windows, you can select only **Common weak passwords**. You can click the detection item name and click **Define** in the list on the right to customize weak password or password complexity detection rules. You can also configure them on the **Baseline Checks** page. For details, see **Defining a Rule to Check Password Complexity Policies** and **Defining Weak Passwords**. For more information, see **Baseline Check Content**.	● **OS**: - ● **Baselines**: Select all.

Step 8 Confirm parameter settings and click **Next**.

Step 9 Select the servers where the policy is to be applied. Click **OK**.

----End

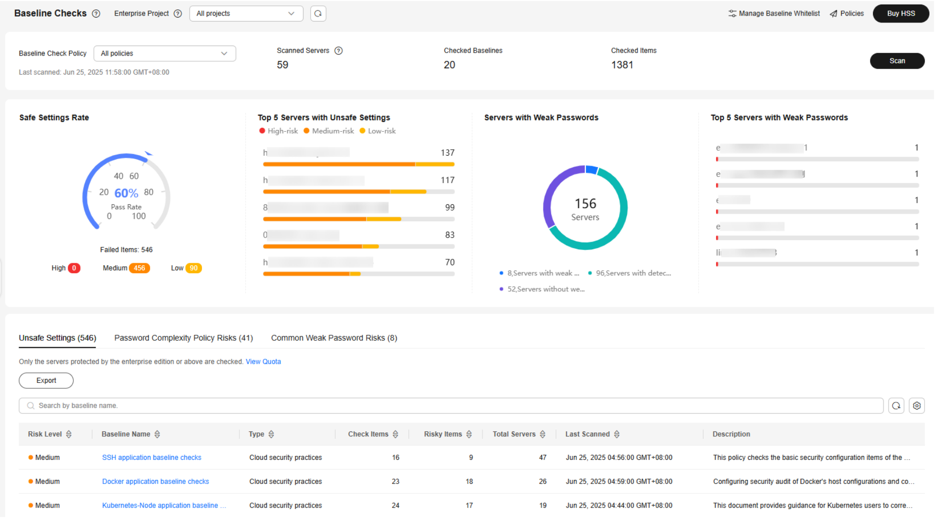
Creating a Custom Check Policy

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

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

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

Figure 5-32 Baseline checks



Baseline Check Policy: All policies

Last scanned: Jun 25, 2025 11:58:00 GMT+08:00

Scanned Servers: 59

Checked Baselines: 20

Checked Items: 1381

Failed Items: 546

High 0 Medium 456 Low 90

Unsafe Settings (546) | Password Complexity Policy Risks (41) | Common Weak Password Risks (8)

Only the servers protected by the enterprise edition or above are checked. View Quota

Search by baseline name.

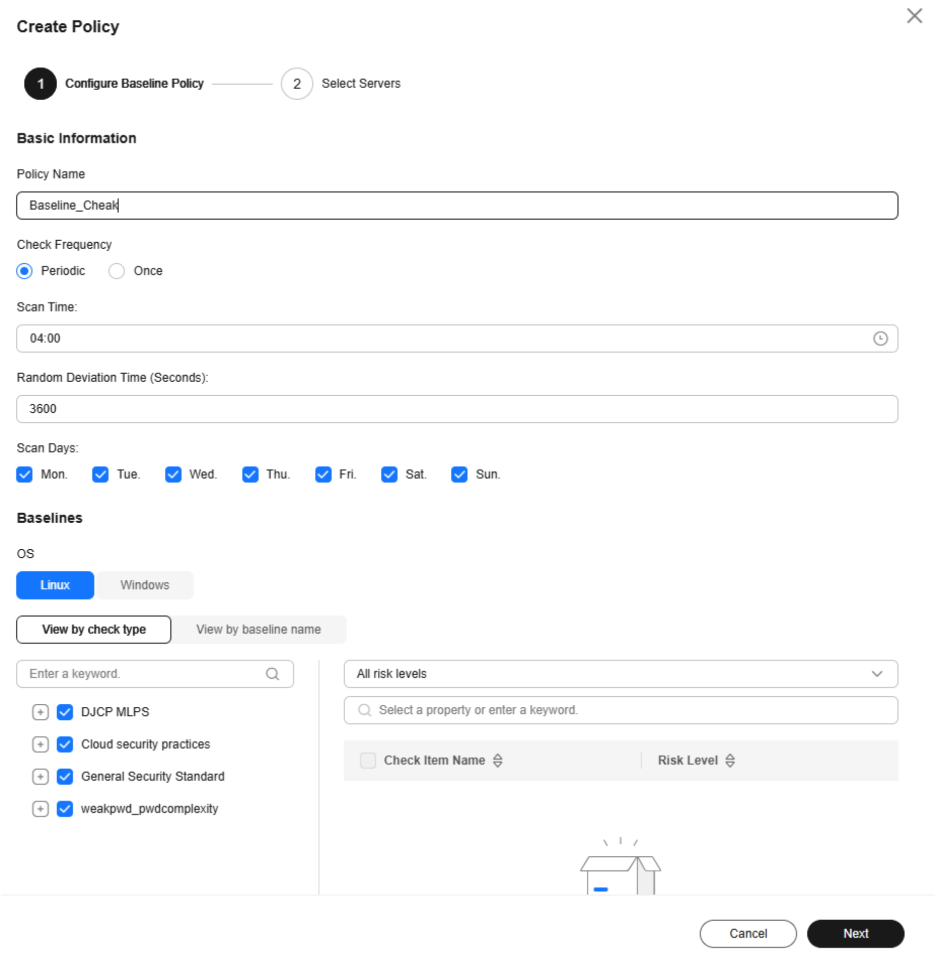
Risk Level	Baseline Name	Type	Check Items	Risky Items	Total Servers	Last Scanned	Description
Medium	SSH application baseline checks	Cloud security practices	16	9	47	Jun 25, 2025 04:56:00 GMT+08:00	This policy checks the basic security configuration items of the ...
Medium	Docker application baseline checks	Cloud security practices	23	18	26	Jun 25, 2025 04:59:00 GMT+08:00	Configuring security audit of Docker's host configurations and co...
Medium	Kubernetes-Node application baseline ...	Cloud security practices	24	17	19	Jun 25, 2025 04:44:00 GMT+08:00	This document provides guidance for Kubernetes users to corre...

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the upper right corner of the page, click **Policies**.

Step 6 Click **Create Policy**. On the **Create Policy** page, configure the baseline check policy as prompted. For more information, see **Table 5-14**.

Figure 5-33 Creating a policy



Create Policy

1 Configure Baseline Policy — 2 Select Servers

Basic Information

Policy Name: Baseline_Cheak

Check Frequency: ● Periodic ○ Once

Scan Time: 04:00

Random Deviation Time (Seconds): 3600

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

Baselines

OS: Linux

View by check type

☑ DJCP MLPS
☑ Cloud security practices
☑ General Security Standard
☑ weakpwd_pwdcomplexity

All risk levels

Table 5-14 Policy parameters

Parameter	Description	Recommended Value
Policy Name	Enter a policy name. The requirements are as follows: ● It can contain 1 to 64 characters. ● It can contain letters, numbers, underscores (_), and hyphens (-).	-
Check Frequency	Set the check frequency of the policy. ● **Periodic**: The check is performed automatically and periodically. ● **Once**: The check is performed manually only once.	Periodic
Scan Time	Click the input box and set the scan time.	04:00

Parameter	Description	Recommended Value
Random Deviation Time (Seconds)	Enter the allowed delay (in seconds) of a scan task. The value must be a positive integer. For example, if the scan time is 04:00 and the random deviation time is 3,600 seconds, the scan task will be performed sometime between 04:00 and 05:00.	3600
Scan Days	Select the days of a week for scans. The options include Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
Baselines	• **OS** Select the server OS type (**Linux** or **Windows**). • **Baseline** Select baselines. You can click **View by check type** or **View by baseline name** to browse faster. – You can select top-level types **DJCP MLPS Compliance**, **Cloud security practices**, **General Security Standard**, and **Weak Password & Password Complexity**. – You can click the ⊞ next to a top-level type to expand level-2 types. – You can click the ⊞ next to a level-2 type to expand level-3 types. – After you click a level-2 or level-3 type, the check items of that type will be displayed in the list on the right. – If you click **Weak Passwords & Password Complexity** (supported for Linux only), you can click **Define** to define the check standard for common weak passwords or password complexity policies. You can also configure them on the **Baseline Checks** page. For details, see **Defining a Rule to Check Password Complexity Policies** and **Defining Weak Passwords**. For more information, see **Baseline Check Content**.	• **OS**: - • **Baselines**: Select all.

Step 7 Confirm parameter settings and click **Next**.

Step 8 Select the servers where the policy is to be applied. Click **OK**.

If the new policy is displayed in the protection policy list, the creation succeeded.

----End

Defining a Rule to Check Password Complexity Policies

While you configure a baseline check policy, you can select whether to check the password complexity policies on servers. This section describes how to modify the rule used for checking password complexity policies.

The rule will be applied to all the baseline check policies under the current enterprise project.

Step 1 Log in to the management console.

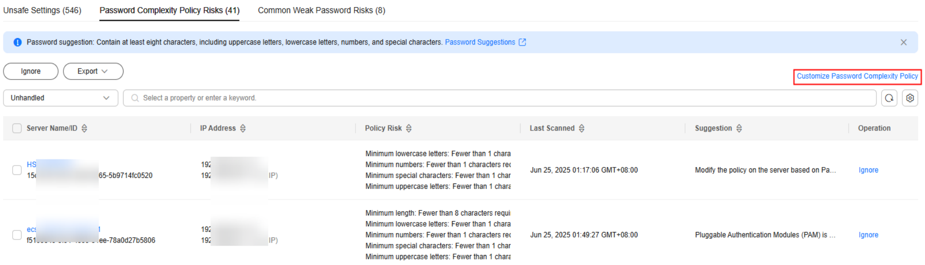
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

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

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 On the **Password Complexity Policy Risks** tab, click **Customize Password Complexity Policy**.

Figure 5-34 Defining a rule to check password complexity policies



Unsafe Settings (546)
Password Complexity Policy Risks (41)
Common Weak Password Risks (8)
Ignore
Export
Customize Password Complexity Policy
Unhandled
Select a property or enter a keyword.

Password suggestion: Contain at least eight characters, including uppercase letters, lowercase letters, numbers, and special characters. Password Suggestions

Server Name/ID	IP Address	Policy Risk	Last Scanned	Suggestion	Operation
HS[redacted] 15[redacted]65-5b9714fc0520	192[redacted] 192[redacted]IP)	Minimum lowercase letters: Fewer than 1 chara Minimum numbers: Fewer than 1 characters re Minimum special characters: Fewer than 1 char Minimum uppercase letters: Fewer than 1 chara	Jun 25, 2025 01:17:06 GMT+08:00	Modify the policy on the server based on Pa...	Ignore
ecs[redacted] f51[redacted]ee-78a0d27b5806	192[redacted] 192[redacted]IP)	Minimum length: Fewer than 8 characters requi Minimum lowercase letters: Fewer than 1 chara Minimum numbers: Fewer than 1 characters re Minimum special characters: Fewer than 1 char Minimum uppercase letters: Fewer than 1 chara	Jun 25, 2025 01:49:27 GMT+08:00	Pluggable Authentication Modules (PAM) is ...	Ignore

Step 6 In the dialog box that is displayed, configure the password complexity policy items, and click **OK**.

The system checks the password complexity against your settings.

----End

Defining Weak Passwords

While you configure a baseline check policy, you can select whether to check for common weak passwords. This section describes how to define weak passwords.

The weak password settings will be applied to all the baseline check policies under the current enterprise project.

Step 1 Log in to the management console.

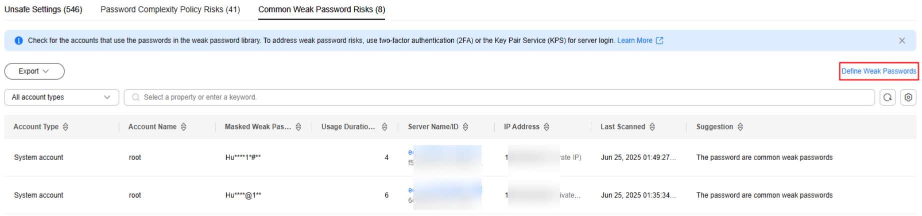
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

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

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 On the **Common Weak Password Risks** tab page, click **Define Weak Passwords**.

Figure 5-35 Defining weak passwords



Unsafe Settings (546) | Password Complexity Policy Risks (41) | Common Weak Password Risks (8)

Check for the accounts that use the passwords in the weak password library. To address weak password risks, use two-factor authentication (2FA) or the Key Pair Service (KPS) for server login. Learn More

Export | Define Weak Passwords

All account types | Select a property or enter a keyword.

Account Type	Account Name	Masked Weak Pas...	Usage Duratio...	Server Name/ID	IP Address	Last Scanned	Suggestion
System account	root	Hu****1*#**	4	e[redacted] f5[redacted]	1[redacted]ate IP)	Jun 25, 2025 01:49:27...	The password are common weak passwords
System account	root	Hu****@1**	6	e[redacted] 6[redacted]	1[redacted]ivate...	Jun 25, 2025 01:35:34...	The password are common weak passwords

Step 6 In the dialog box that is displayed, enter weak passwords and click **OK**.

HSS will check for the weak passwords you defined in addition to common weak passwords.

----End

5.2.3 Performing a Baseline Check

Scenarios

You can perform a check immediately or schedule it for later.

- Scheduled check: HSS periodically performs baseline checks based on the scheduled check policy you configured. For more information, see Configuring a Baseline Check Policy.
- One-time manual check: You can manually start a baseline check to learn the server security status in real time.

This topic describes how to manually start a baseline check.

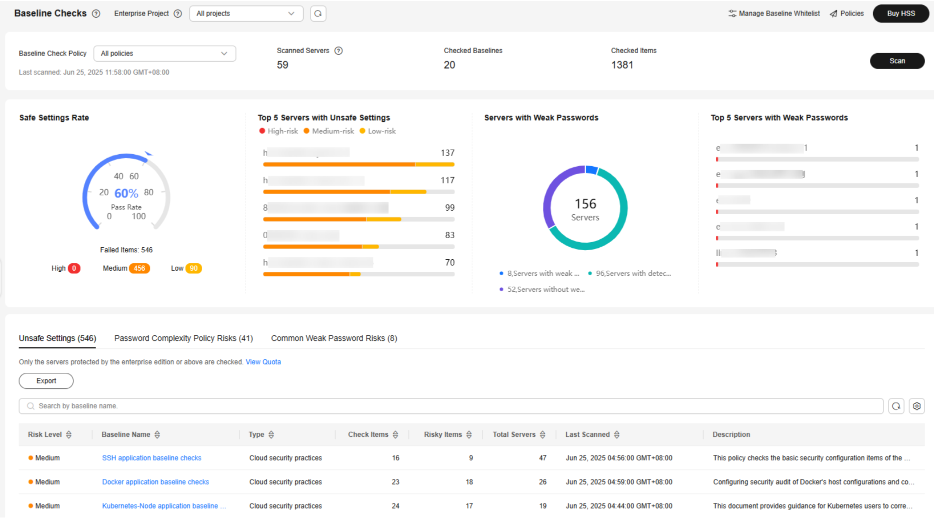
Manually Performing a Baseline Check

Step 1 Log in to the management console.

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

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

Figure 5-36 Baseline checks



Baseline Check Policy: All policies

Last scanned: Jun 25, 2025 11:58:00 GMT+08:00

Scanned Servers: 59

Checked Baselines: 20

Checked Items: 1381

Failed Items: 546

Only the servers protected by the enterprise edition or above are checked. View Quota

Risk Level	Baseline Name	Type	Check Items	Risky Items	Total Servers	Last Scanned	Description
● Medium	SSH application baseline checks	Cloud security practices	16	9	47	Jun 25, 2025 04:56:00 GMT+08:00	This policy checks the basic security configuration items of the ...
● Medium	Docker application baseline checks	Cloud security practices	23	18	26	Jun 25, 2025 04:59:00 GMT+08:00	Configuring security audit of Docker's host configurations and co...
● Medium	Kubernetes-Node application baseline ...	Cloud security practices	24	17	19	Jun 25, 2025 04:44:00 GMT+08:00	This document provides guidance for Kubernetes users to corre...

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 In the upper right corner of the page, click **Scan**.

Step 6 Select a policy and click **OK**.

To view or modify the policy details, click **Policies** in the upper right corner of the **Baseline Checks** page. On the displayed page, click **Edit** in the **Operation** column of a policy.

Step 7 If the time displayed in the **Last scanned** area under the **Baseline Check Policy** drop-down list changes to the actual check time, the check has completed.

After a manual check is performed, the button will display **Scanning** and be disabled. If the check time exceeds 30 minutes, the button will be automatically enabled again. If the time displayed in the **Last scanned** area becomes the current check time, it indicates the check has completed.

After the check is complete, you can view the check results and handling suggestions by referring to **Viewing and Handling Baseline Check Results**.

----End

5.2.4 Viewing and Handling Baseline Check Results

Scenarios

You can check for and fix unsafe baseline settings, weak passwords, and insecure password complexity policies on your servers.

Constraints

Only the HSS enterprise, premium, WTP, and container editions support baseline configuration checks.

Detection Description

The MySQL baseline detection of Linux OS is based on the MySQL 5 security configuration specifications. If MySQL 8 is installed on your server, the following check items are not displayed in the detection results, because they are discarded in that version. The detection results are displayed only on the server whose MySQL version is 5.

- Rule: Do not set **old_passwords** to **1**.
- Rule: Set secure_auth to **1** or **ON**.
- Rule: Do not set **skip_secure_auth**.
- Rule: Set **log_warnings** to **2**.
- Rule: Configure the MySQL binlog clearing policy.
- Rule: The **sql_mode** parameter contains **NO_AUTO_CREATE_USER**.
- Rule: Use the MySQL audit plug-in.

Viewing Baseline Check Overview Information

Step 1 Log in to the management console.

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

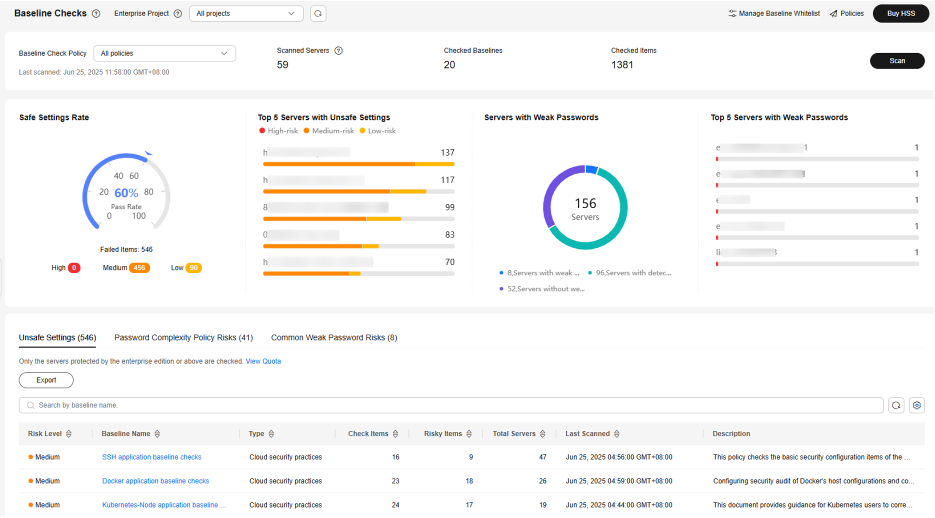
Step 3 In the navigation pane on the left, choose **Risk Management** > **Baseline Checks**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click different tabs on the displayed page to check the detected unsafe settings. Table 5-15 lists the corresponding parameters.

To view the check results of servers under different baseline check policies, you can switch between baseline check policies.

Figure 5-37 Baseline checks



Baseline Check Policy: All policies

Last scanned: Jun 25, 2025 11:58:00 GMT+08:00

Scanned Servers: 59

Checked Baselines: 20

Checked Items: 1381

Failed Items: 546

Only the servers protected by the enterprise edition or above are checked. View Quota

Risk Level	Baseline Name	Type	Check Items	Risky Items	Total Servers	Last Scanned	Description
Medium	SSH application baseline checks	Cloud security practices	16	9	47	Jun 25, 2025 04:56:00 GMT+08:00	This policy checks the basic security configuration items of the ...
Medium	Docker application baseline checks	Cloud security practices	23	18	26	Jun 25, 2025 04:59:00 GMT+08:00	Configuring security audit of Docker's host configurations and co...
Medium	Kubernetes-Node application baseline ...	Cloud security practices	24	17	19	Jun 25, 2025 04:44:00 GMT+08:00	This document provides guidance for Kubernetes users to corre...

Table 5-15 Baseline check overview

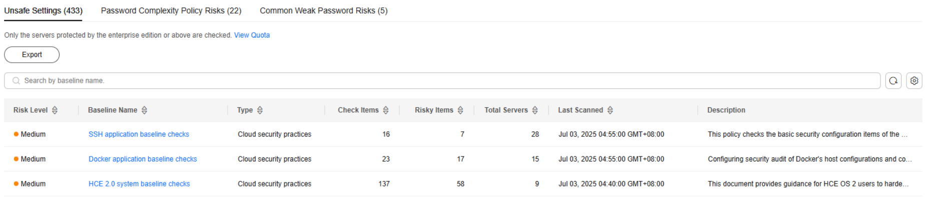
Parameter	Description
Baseline Check Policy	Available baseline check policies that have been added. You can select, create, edit, and delete these policies.
Scanned Servers	Total number of detected servers.
Checked Baselines	Number of baselines executed during the server detection.
Checked Items	Total number of checked server configuration items.
Safe Settings Rate	Percentage of configuration items that passed the baseline check to the total number of check items. Failed items are displayed by risk level.
Top 5 Servers with Unsafe Settings	Statistics on servers with server configuration risks. The top 5 servers with the highest risks are preferentially sorted. If no high-risk settings exist, the servers are sorted into medium-risk and low-risk ones in sequence.
Servers with Weak Passwords	Total number of detected servers, as well as the numbers of servers with weak passwords, those without weak passwords, and those with weak password detection disabled.
Top 5 Servers with Weak Passwords	Statistics on the top 5 servers with most weak password risks.
Unsafe Settings	Alarms generated for servers with configuration risks and the risk statistics.
Password Complexity Policy Risks	Statistics on the servers whose password complexity policies do not meet the baseline requirements.
Common Weak Password Risks	Statistics on servers with weak passwords and accounts.

----End

Viewing and Handling Baseline Configuration Risks

Step 1 Click the **Unsafe Settings** tab to view the server baseline risks. For more information, see **Table 5-16**.

Figure 5-38 Viewing baseline configuration risks



Unsafe Settings (433)
Password Complexity Policy Risks (22)
Common Weak Password Risks (5)

Only the servers protected by the enterprise edition or above are checked. View Quota

Export
Search by baseline name.

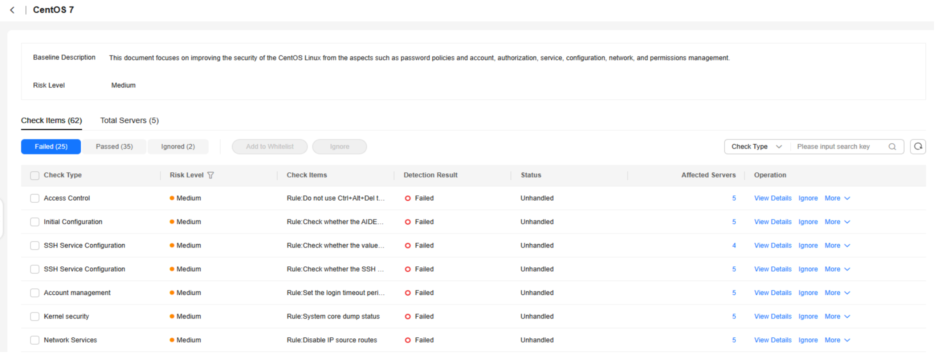
Risk Level	Baseline Name	Type	Check Items	Risky Items	Total Servers	Last Scanned	Description
● Medium	SSH application baseline checks	Cloud security practices	16	7	28	Jul 03, 2025 04:55:00 GMT+08:00	This policy checks the basic security configuration items of the ...
● Medium	Docker application baseline checks	Cloud security practices	23	17	15	Jul 03, 2025 04:55:00 GMT+08:00	Configuring security audit of Docker's host configurations and co...
● Medium	HCE 2.0 system baseline checks	Cloud security practices	137	58	9	Jul 03, 2025 04:40:00 GMT+08:00	This document provides guidance for HCE OS 2 users to harde...

Table 5-16 Baseline parameters

Parameter	Description
Risk Level	Level of a detection result. ● High ● Low ● Medium ● Secure
Baseline Name	Name of the baseline that is checked.
Type	Policy type of the baseline that has been checked. ● Cloud security practices ● DJCP MLPS ● General security standard
Check Item	Total number of configuration items that are checked.
Risky Item	Total number of the risky configurations.
Scanned Servers	Total number of servers scanned against a baseline.
Last Scanned	Time when the last detection was performed.
Description	Description of a baseline.

Step 2 Click a baseline name in the list to view the baseline description, scanned servers, and details about all check items.

Figure 5-39 Viewing baseline check details



< | CentOS 7

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

Risk Level: Medium

Check Type	Risk Level	Check Items	Detection Result	Status	Affected Servers	Operation
□ Access Control	● Medium	Rule:Do not use Ctrl+Alt+Del t...	○ Failed	Unhandled	5	View Details Ignore More
□ Initial Configuration	● Medium	Rule:Check whether the AIDE...	○ Failed	Unhandled	5	View Details Ignore More
□ SSH Service Configuration	● Medium	Rule:Check whether the value...	○ Failed	Unhandled	4	View Details Ignore More
□ SSH Service Configuration	● Medium	Rule:Check whether the SSH ...	○ Failed	Unhandled	5	View Details Ignore More
□ Account management	● Medium	Rule:Set the login timeout peri...	○ Failed	Unhandled	5	View Details Ignore More
□ Kernel security	● Medium	Rule:System core dump status	○ Failed	Unhandled	5	View Details Ignore More
□ Network Services	● Medium	Rule:Disable IP source routes	○ Failed	Unhandled	5	View Details Ignore More

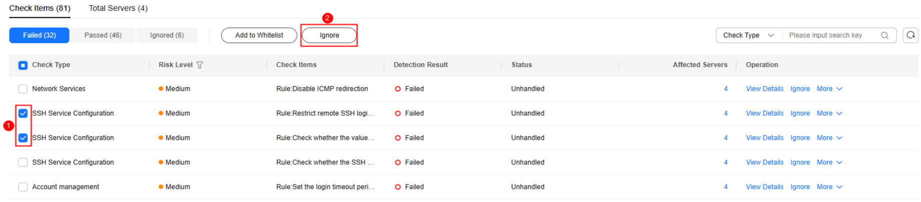
Step 3 Handle risk items.

- **Ignoring risks**

After a risk is ignored, it will be displayed in the ignored item list. It will no longer be reported in the HSS baseline checks on servers.

a. Click **Ignore** in the **Operation** column of a check item to ignore it. Select multiple check items and click **Ignore** to ignore them in batches.

Figure 5-40 Ignoring risks



■ Check Type	Risk Level	Check Items	Detection Result	Status	Affected Servers	Operation
□ Network Services	● Medium	Rule:Disable ICMP redirection	○ Failed	Unhandled	4	View Details Ignore More
☑ SSH Service Configuration	● Medium	Rule:Restrict remote SSH logi...	○ Failed	Unhandled	4	View Details Ignore More
☑ SSH Service Configuration	● Medium	Rule:Check whether the value...	○ Failed	Unhandled	4	View Details Ignore More
□ SSH Service Configuration	● Medium	Rule:Check whether the SSH ...	○ Failed	Unhandled	4	View Details Ignore More
□ Account management	● Medium	Rule:Set the login timeout peri...	○ Failed	Unhandled	4	View Details Ignore More

b. In the displayed dialog box, click **OK**.

   You can click **Ignored** above the check item list to view the ignored items.

- **Fixing risks**

  a. Click **View Details** in the **Operation** column of a risk item.

  b. View the content in the **Audit Description**, **Suggestion**, and **Affected Servers**. Rectify the unsafe settings.

  NOTE

  - Currently, one-click fixing is supported for some EulerOS baseline configurations and CentOS 8 baseline configurations. You can simply click **Fix** in the **Operation** column of the target EulerOS or CentOS check item to fix the unsafe settings. If some parameters need to be configured during restoration, retain the default values.
  - You are advised to fix the settings with high severity immediately and fix those with medium or low severity.

  c. After the repair is complete, click **Verify** on the **Affected Servers** tab page to verify the result.

  If a failed check item has been fixed, you can update its status through verification. The restrictions are as follows:

  - Currently, baseline verification is not supported for Windows OSs.
  - The agent status of the target server must be online.
  - Only one risk item can be verified at a time. Other risk items can be verified only after the risk items are verified.
  - Baseline checks are supported for the following Linux OSs: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 7, CentOS 8, EulerOS, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, SUSE 12, SUSE 15, HCE 1.1, and HCE 2.0.

  d. Click **OK** to start the verification.

  e. Return to the check item list page and view the status of the risk item.

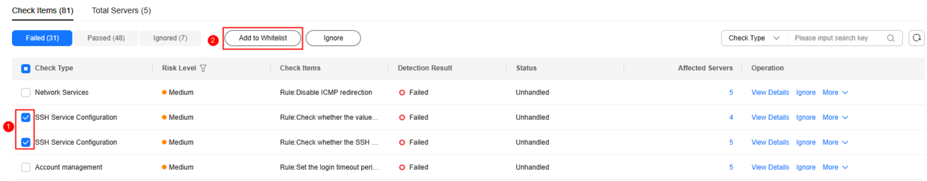
  The status changes to **Verifying**. The system starts automatic verification. After the verification is complete, check the status. If a check item failed to be fixed, click **View Cause** to view the cause. Then, fix it again.

- **Whitelisting a risk**

  Whitelisted risk items will be displayed in the whitelist. In later baseline checks, HSS will not check for them.

  a. Click **Add to Whitelist** in the **Operation** column of a check item. Select multiple check items and click **Ignore** to ignore them in batches.

  Figure 5-41 Adding an item to whitelist



Check Items (81) Total Servers (5)

Failed (31) Passed (48) Ignored (7) 2 Add to Whitelist Ignore Check Type Please input search key

Check Type	Risk Level	Check Items	Detection Result	Status	Affected Servers	Operation
□ Network Services	● Medium	Rule:Disable ICMP redirection	○ Failed	Unhandled	5	View Details Ignore More
☑ SSH Service Configuration	● Medium	Rule:Check whether the value...	○ Failed	Unhandled	4	View Details Ignore More
☑ SSH Service Configuration	● Medium	Rule:Check whether the SSH ...	○ Failed	Unhandled	5	View Details Ignore More
□ Account management	● Medium	Rule:Set the login timeout peri...	○ Failed	Unhandled	5	View Details Ignore More

  b. On the **Add to Whitelist** page, confirm the server information, configure **Add to global whitelist** as needed, and add remarks.

  To exclude the whitelisted items from checks for all servers, select **Add to global whitelist**.

  c. Click **OK**.

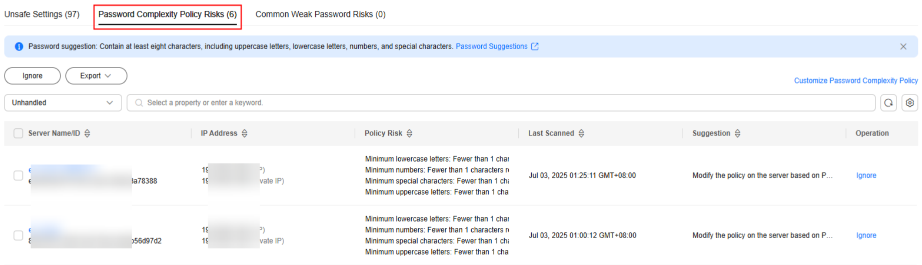
  To check whitelisted items, return to the **Baseline Checks** page and click **Manage Baseline Whitelist** in the upper right corner. For more information, see **Managing the Baseline Whitelist**.

----End

Checking and Handling Password Complexity Policy Risks

Step 1 Click the **Password Complexity Policy Risks** tab to view the risk statistical items and handling suggestions. For more information, see **Table 5-17**.

Figure 5-42 Viewing password complexity policy risks



Unsafe Settings (97) Password Complexity Policy Risks (6) Common Weak Password Risks (0)

Password suggestion: Contain at least eight characters, including uppercase letters, lowercase letters, numbers, and special characters. Password Suggestions

Ignore Export Customize Password Complexity Policy

Unhandled Select a property or enter a keyword.

Server Name/ID	IP Address	Policy Risk	Last Scanned	Suggestion	Operation
□ [redacted]a78388	[redacted]) [redacted]vate IP)	Minimum lowercase letters: Fewer than 1 char Minimum numbers: Fewer than 1 characters r Minimum special characters: Fewer than 1 ch Minimum uppercase letters: Fewer than 1 cha	Jul 03, 2025 01:25:11 GMT+08:00	Modify the policy on the server based on P...	Ignore
□ [redacted]56d97d2	[redacted]) [redacted]vate IP)	Minimum lowercase letters: Fewer than 1 char Minimum numbers: Fewer than 1 characters r Minimum special characters: Fewer than 1 ch Minimum uppercase letters: Fewer than 1 cha	Jul 03, 2025 01:00:12 GMT+08:00	Modify the policy on the server based on P...	Ignore

Table 5-17 Parameters for password complexity policy risks

Parameter	Description
Server Name/ID	The name and ID of a checked server.
IP Address	The EIP and private IP address of a checked server.

Parameter	Description
Policy Risk	The password complexity policy settings that do not meet security requirements.
Last Scanned	Last time when the password complexity policy was checked.
Suggestion	Suggestions for modifying the password complexity policy.

Step 2 Handle password complexity policy check results.

- Modifying the password complexity policy

  a. Modify the password complexity policy on the server based on the **Suggestion** column in the check result.

     - To monitor the password complexity policy on a Linux server, install the Pluggable Authentication Modules (PAM) on the server. For details, see **How Do I Install a PAM in a Linux OS?**

     - For details about how to modify the password complexity policy on a Linux server, see **How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS?**

     - For details about how to modify the password complexity policy on a Windows server, see **How Do I Set a Secure Password Complexity Policy in a Windows OS?**

  b. Save the modification. Click **Scan** in the upper part of the **Baseline Checks** page to verify the modification.

     If you do not perform a manual verification, HSS will automatically check the settings at 00:00:00 the next day.

- **Ignoring password complexity policy check results**

  You can view the ignored detection results on the **Ignored** tab page.

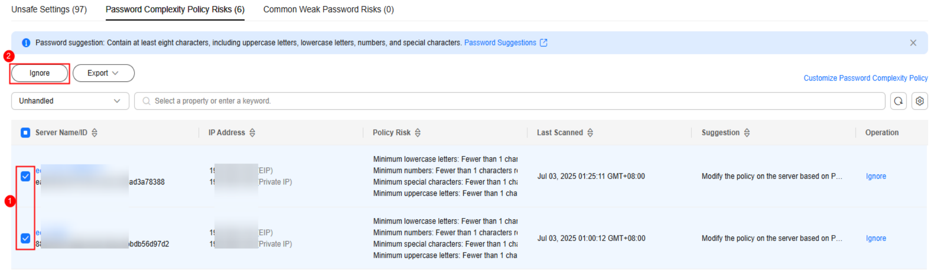
  – Ignoring a single result

    In the **Operation** column of a server scan result, click **Ignore**.

  – Batch ignoring records

    Select scan results and click **Ignore** in the upper left corner of the list. Up to 200 results can be ignored at a time.

Figure 5-43 Ignoring multiple results



Unsafe Settings (97)
Password Complexity Policy Risks (6)
Common Weak Password Risks (0)
Ignore
Export
Customize Password Complexity Policy
Unhandled
Select a property or enter a keyword.
1
2

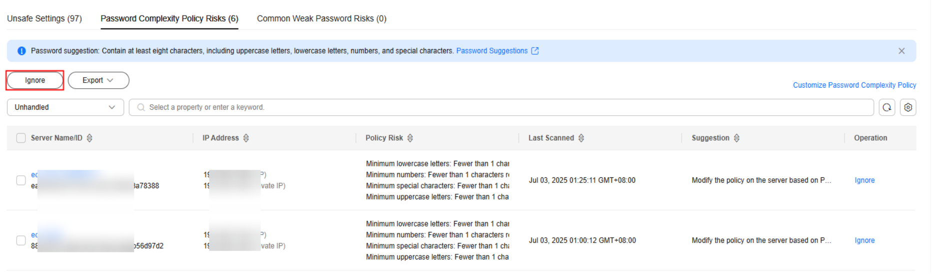
Password suggestion: Contain at least eight characters, including uppercase letters, lowercase letters, numbers, and special characters. Password Suggestions

☐ Server Name/ID	IP Address	Policy Risk	Last Scanned	Suggestion	Operation
☑ e[redacted] e[redacted]ad3a78388	1[redacted]EIP) 1[redacted]Private IP)	Minimum lowercase letters: Fewer than 1 char Minimum numbers: Fewer than 1 characters r Minimum special characters: Fewer than 1 ch Minimum uppercase letters: Fewer than 1 cha	Jul 03, 2025 01:25:11 GMT+08:00	Modify the policy on the server based on P...	Ignore
☑ e[redacted] 8[redacted]bdb56d97d2	1[redacted]EIP) 1[redacted]Private IP)	Minimum lowercase letters: Fewer than 1 char Minimum numbers: Fewer than 1 characters r Minimum special characters: Fewer than 1 ch Minimum uppercase letters: Fewer than 1 cha	Jul 03, 2025 01:00:12 GMT+08:00	Modify the policy on the server based on P...	Ignore

– Ignoring all results

Click **Ignore** in the upper left corner of the list. Up to 1000 password complexity policy check results can be ignored at a time.

Figure 5-44 Ignoring all results


Unsafe Settings (97)
Password Complexity Policy Risks (6)
Common Weak Password Risks (0)
Ignore
Export
Customize Password Complexity Policy
Unhandled
Select a property or enter a keyword.

Password suggestion: Contain at least eight characters, including uppercase letters, lowercase letters, numbers, and special characters. Password Suggestions

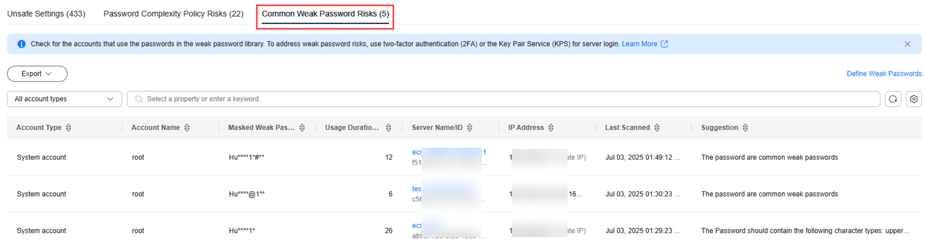
Server Name/ID	IP Address	Policy Risk	Last Scanned	Suggestion	Operation
ec[redacted] ea[redacted]a78388	19[redacted]P) 19[redacted]vate IP)	Minimum lowercase letters: Fewer than 1 char Minimum numbers: Fewer than 1 characters r Minimum special characters: Fewer than 1 ch Minimum uppercase letters: Fewer than 1 cha	Jul 03, 2025 01:25:11 GMT+08:00	Modify the policy on the server based on P...	Ignore
ec[redacted] 88[redacted]b56d97d2	19[redacted]P) 19[redacted]vate IP)	Minimum lowercase letters: Fewer than 1 char Minimum numbers: Fewer than 1 characters r Minimum special characters: Fewer than 1 ch Minimum uppercase letters: Fewer than 1 cha	Jul 03, 2025 01:00:12 GMT+08:00	Modify the policy on the server based on P...	Ignore

----End

Viewing and Handling Common Weak Password Risks

Step 1 Click the **Common Weak Password Risks** tab to view the statistics of weak passwords on the server. For more information, see **Table 5-18**.

Figure 5-45 Viewing common weak password risks


Unsafe Settings (433)
Password Complexity Policy Risks (22)
Common Weak Password Risks (5)
Export
Define Weak Passwords
All account types
Select a property or enter a keyword.

Check for the accounts that use the passwords in the weak password library. To address weak password risks, use two-factor authentication (2FA) or the Key Pair Service (KPS) for server login. Learn More

Account Type	Account Name	Masked Weak Pas...	Usage Duratio...	Server Name/ID	IP Address	Last Scanned	Suggestion
System account	root	Hu****1*#**	12	ecs[redacted]1 f51[redacted]...	1[redacted]ate IP)	Jul 03, 2025 01:49:12 ...	The password are common weak passwords
System account	root	Hu****@1**	6	tes[redacted] c56[redacted]...	1[redacted]16...	Jul 03, 2025 01:30:23 ...	The password are common weak passwords
System account	root	Hu****1*	26	ecs[redacted] ab[redacted]...	1[redacted]ate IP)	Jul 03, 2025 01:29:23 ...	The Password should contain the following character types: upper...

Table 5-18 Parameters for common weak password risks

Parameter	Description
Account Type	Type of an account.
Account Name	Accounts identified with weak passwords.

Parameter	Description
Masked Weak Password	Masking result of a weak password. The rules for displaying masked weak passwords are as follows: ● ************ indicates that the password length is less than 8. ● *****a****** indicates that the password contains only lowercase letters. ● *****B***** indicates that the password contains only uppercase letters. ● ****a**B**** indicates that the password contains only uppercase and lowercase letters. ● ****a**A***@**1**** indicates that the password is a common weak password.
Usage Duration (Days)	Duration a weak password is used.
Server Name/ID	Name and ID of the server where a weak password is used.
IP Address	The EIP and private IP address of a server.
Last Scanned	Time when the last scan completed.
Suggestion	Suggestion for changing weak passwords. You can check why the password is regarded insecure and set a strong password based on the suggestion.

Step 2 Log in to the server and change the weak password.

NOTE

- To enhance server security, you are advised to modify the accounts with weak passwords in a timely manner, such as SSH accounts.
- To protect internal data of your server, you are advised to modify software accounts that use weak passwords, such as MySQL accounts and FTP accounts.
- A password should contain more than eight characters, including uppercase letters, lowercase letters, digits, and special characters.

Step 3 After the weak password is changed, perform a manual check in the upper part of the **Baseline Checks** page to verify the result.

If you do not perform a manual verification, HSS will automatically check the settings at 00:00:00 the next day.

----End

5.2.5 Exporting a Baseline Check Report

Scenarios

Yon can export the baseline check results to your local PC.

Constraints

Only the HSS enterprise, premium, WTP, and container editions support baseline configuration checks.

Exporting a Baseline Check Report

Step 1 Log in to the management console.

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

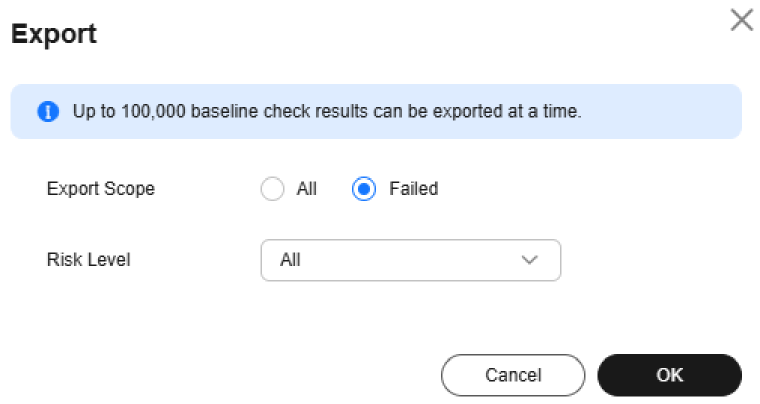
Step 3 In the navigation pane on the left, choose **Risk Management** > **Baseline Checks**.

----End

Step 1 Perform the following operations to export the check results based on the baseline check type:

- **Unsafe Settings**
  a. Click the **Unsafe Settings** tab and click **Export** in the upper left corner of the tab page.
  b. In the dialog box that is displayed, set **Export Scope** and **Risk Level**, and click **OK**.
     - **Export Scope**: Select all data, or only the settings that failed to pass the check.
     - **Risk Level**: Select **All**, **High**, **Medium**, **Low**, or **Safe**.

Figure 5-46 Exporting baseline check results



Export

Up to 100,000 baseline check results can be exported at a time.

Export Scope ○ All ● Failed

Risk Level All

- **Password Complexity Policy Risks**

  Click the **Password Complexity Policy Risks** tab. In the upper left corner of the list, click **Export**.

- **Common Weak Password Risks**

  Click the **Common Weak Password Risks** tab. In the upper left corner of the list, click **Export** to export check results.

You can enter the server name, IP address, or account name in the upper right corner of the list, and press **Enter** to search for and download the results.

----End

5.2.6 Managing the Baseline Whitelist

Scenarios

You can add the baseline check items under **DJCP MLPS**, **Cloud security practices**, or **General Security Standard** to the whitelist. HSS will not check the whitelisted items on servers.

- **Creating a Baseline Whitelist**

  You can add check items to the whitelist while **handling configuration check results**. You can also create a baseline whitelist and add check items and servers to it.

- **Editing a Baseline Whitelist**

  You can edit an existing baseline whitelist to modify the whitelisted servers.

- **Deleting a Baseline Whitelist**

  To resume checks for an item, remove it from the baseline whitelist.

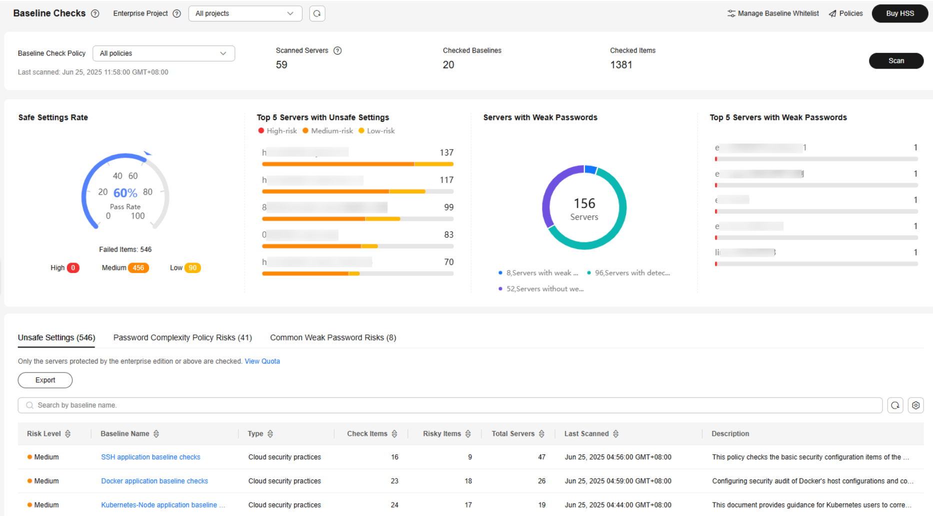
Creating a Baseline Whitelist

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

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

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

Figure 5-47 Baseline checks



Baseline Check Policy: All policies

Last scanned: Jun 25, 2025 11:58:00 GMT+08:00

Scanned Servers: 59

Checked Baselines: 20

Checked Items: 1381

Only the servers protected by the enterprise edition or above are checked.

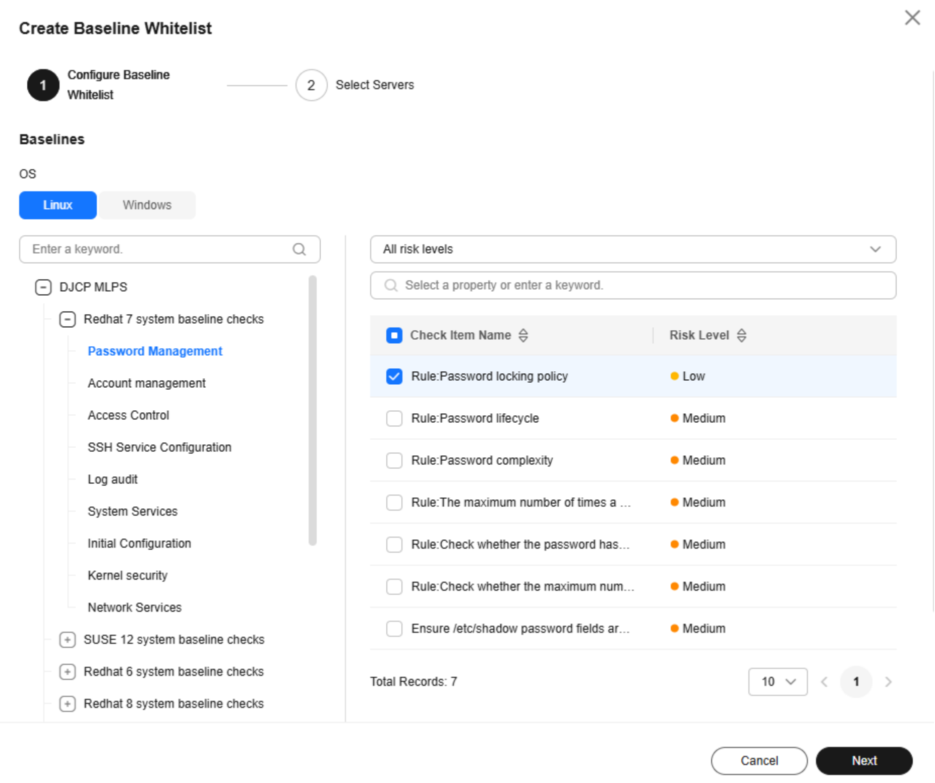
Risk Level	Baseline Name	Type	Check Items	Risky Items	Total Servers	Last Scanned	Description
● Medium	SSH application baseline checks	Cloud security practices	16	9	47	Jun 25, 2025 04:56:00 GMT+08:00	This policy checks the basic security configuration items of the ...
● Medium	Docker application baseline checks	Cloud security practices	23	18	26	Jun 25, 2025 04:59:00 GMT+08:00	Configuring security audit of Docker's host configurations and co...
● Medium	Kubernetes-Node application baseline ...	Cloud security practices	24	17	19	Jun 25, 2025 04:44:00 GMT+08:00	This document provides guidance for Kubernetes users to corre...

Step 4 In the upper right corner of the page, click **Manage Baseline Whitelist**.

Step 5 Click the **Create Whitelist**.

Step 6 Select baseline items and click **Next**. For details, see **Table 5-19**.

Figure 5-48 Creating a baseline whitelist



Create Baseline Whitelist

1 Configure Baseline Whitelist — 2 Select Servers

Baselines

OS

Linux | Windows

Enter a keyword.

- ⊟ DJCP MLPS
  - ⊟ Redhat 7 system baseline checks
    - Password Management
    - Account management
    - Access Control
    - SSH Service Configuration
    - Log audit
    - System Services
    - Initial Configuration
    - Kernel security
    - Network Services
  - ⊞ SUSE 12 system baseline checks
  - ⊞ Redhat 6 system baseline checks
  - ⊞ Redhat 8 system baseline checks

All risk levels

Select a property or enter a keyword.

	Check Item Name	Risk Level
☑	Rule:Password locking policy	● Low
□	Rule:Password lifecycle	● Medium
□	Rule:Password complexity	● Medium
□	Rule:The maximum number of times a ...	● Medium
□	Rule:Check whether the password has...	● Medium
□	Rule:Check whether the maximum num...	● Medium
□	Ensure /etc/shadow password fields ar...	● Medium

Total Records: 7   10   < 1 >

Cancel   Next

Table 5-19 Parameters for creating a baseline whitelist

Parameter	Description
OS	Select the server OS whose check items need to be whitelisted. ● Linux ● Windows
Baseline	Select the baseline items to be whitelisted. Perform the following steps: 1. Click ⊞ next to **DJCP MLPS**, **Cloud security practices**, or **General Security Standard** to expand the level-2 types. 2. Click ⊞ next to a level-2 check type to expand level-3 check types. 3. Click a level-3 check type to view its check items in the list on the right. 4. Select the items to be whitelisted.

Step 7 Select the scope of servers where the whitelist is to be applied.

- **All**: All servers, including those added later.

- **Specific servers**: Select servers.

Step 8 Click **OK**.

You can view the new baseline whitelist in the whitelist table.

----End

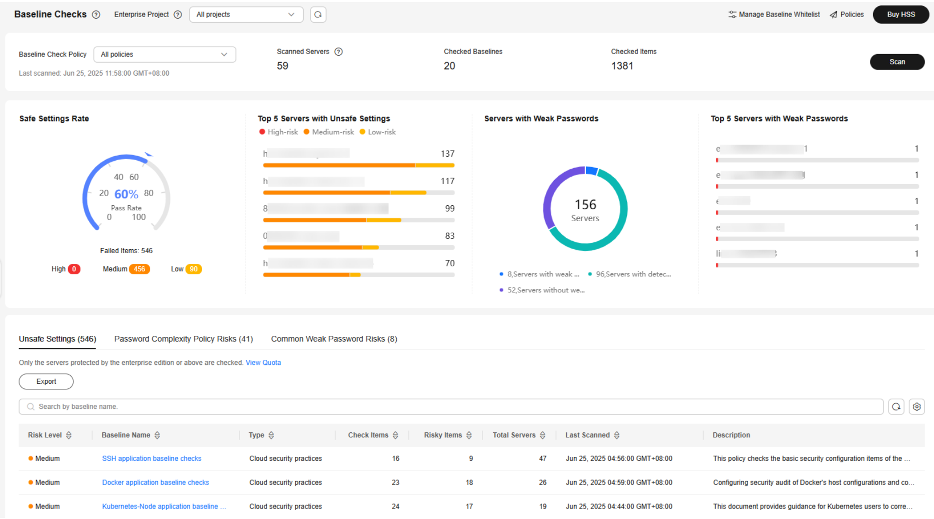
Editing a Baseline Whitelist

Step 1 Log in to the management console.

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

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

Figure 5-49 Baseline checks



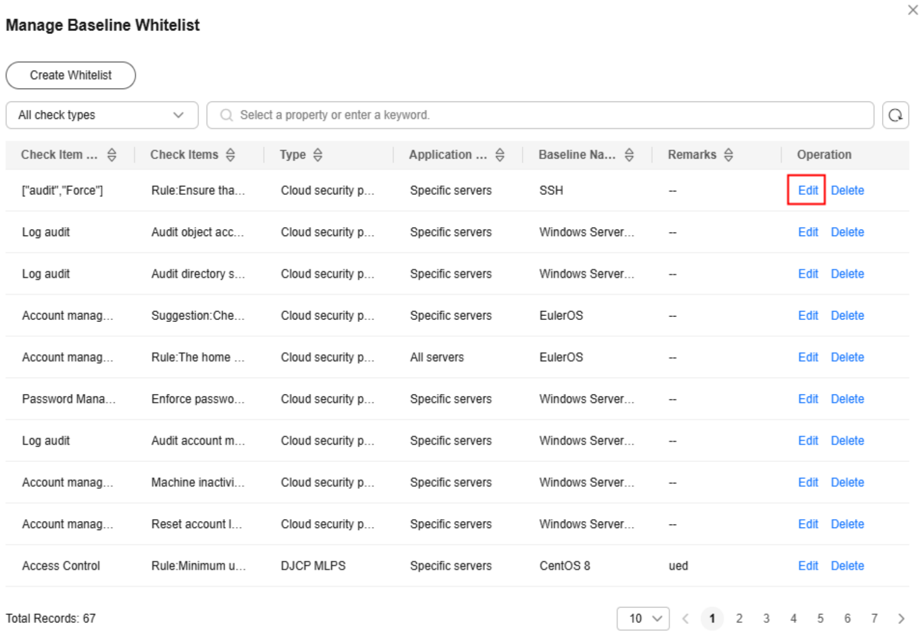
Only the servers protected by the enterprise edition or above are checked. View Quota

Risk Level	Baseline Name	Type	Check Items	Risky Items	Total Servers	Last Scanned	Description
● Medium	SSH application baseline checks	Cloud security practices	16	9	47	Jun 25, 2025 04:56:00 GMT+08:00	This policy checks the basic security configuration items of the ...
● Medium	Docker application baseline checks	Cloud security practices	23	18	26	Jun 25, 2025 04:59:00 GMT+08:00	Configuring security audit of Docker's host configurations and co...
● Medium	Kubernetes-Node application baseline ...	Cloud security practices	24	17	19	Jun 25, 2025 04:44:00 GMT+08:00	This document provides guidance for Kubernetes users to corre...

Step 4 In the upper right corner of the page, click **Manage Baseline Whitelist**.

Step 5 In the **Operation** column of a baseline whitelist, click **Edit**. Modify the whitelist on the edit page.

Figure 5-50 Editing a baseline whitelist



Manage Baseline Whitelist

Check Item ...	Check Items	Type	Application ...	Baseline Na...	Remarks	Operation
["audit","Force"]	Rule:Ensure tha...	Cloud security p...	Specific servers	SSH	--	Edit Delete
Log audit	Audit object acc...	Cloud security p...	Specific servers	Windows Server...	--	Edit Delete
Log audit	Audit directory s...	Cloud security p...	Specific servers	Windows Server...	--	Edit Delete
Account manag...	Suggestion:Che...	Cloud security p...	Specific servers	EulerOS	--	Edit Delete
Account manag...	Rule:The home ...	Cloud security p...	All servers	EulerOS	--	Edit Delete
Password Mana...	Enforce passwo...	Cloud security p...	Specific servers	Windows Server...	--	Edit Delete
Log audit	Audit account m...	Cloud security p...	Specific servers	Windows Server...	--	Edit Delete
Account manag...	Machine inactivi...	Cloud security p...	Specific servers	Windows Server...	--	Edit Delete
Account manag...	Reset account l...	Cloud security p...	Specific servers	Windows Server...	--	Edit Delete
Access Control	Rule:Minimum u...	DJCP MLPS	Specific servers	CentOS 8	ued	Edit Delete

Total Records: 67

Step 6 Select the scope of servers where the whitelist is to be applied.

- **All**: All servers, including those added later.
- **Specific servers**: Select servers.

Step 7 Click **OK**.

----End

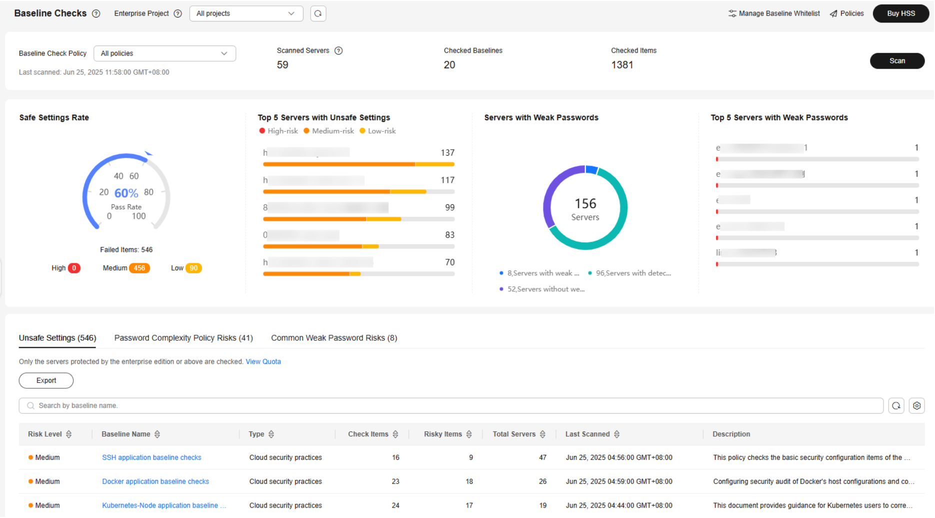
Deleting a Baseline Whitelist

Step 1 Log in to the management console.

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

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

Figure 5-51 Baseline checks



Baseline Check Policy: All policies

Last scanned: Jun 25, 2025 11:58:00 GMT+08:00

Scanned Servers: 59

Checked Baselines: 20

Checked Items: 1381

Failed Items: 546

High 0 Medium 456 Low 90

Unsafe Settings (546) Password Complexity Policy Risks (41) Common Weak Password Risks (8)

Only the servers protected by the enterprise edition or above are checked. View Quota

Search by baseline name.

Risk Level	Baseline Name	Type	Check Items	Risky Items	Total Servers	Last Scanned	Description
● Medium	SSH application baseline checks	Cloud security practices	16	9	47	Jun 25, 2025 04:56:00 GMT+08:00	This policy checks the basic security configuration items of the ...
● Medium	Docker application baseline checks	Cloud security practices	23	18	26	Jun 25, 2025 04:59:00 GMT+08:00	Configuring security audit of Docker's host configurations and co...
● Medium	Kubernetes-Node application baseline ...	Cloud security practices	24	17	19	Jun 25, 2025 04:44:00 GMT+08:00	This document provides guidance for Kubernetes users to corre...

Step 4 In the upper right corner of the page, click **Manage Baseline Whitelist**.

Step 5 In the **Operation** column of a baseline whitelist, click **Delete**.

Step 6 In the dialog box displayed, click **OK**.

----End

5.3 Container Image Security

5.3.1 Container Image Security Overview

What Is an Image?

An image is a standard format for packaging containerized applications. It is used to create containers. An image is like a special file system. It contains the programs, libraries, resources, configuration files, and parameters (including anonymous volumes, environment variables, and users) required for a runtime. An image does not contain any dynamic data, and its content is unchangeable after creation. When deploying a containerized application, you can use an image from Harbor, container image service, or your private image repository.

What Is Container Image Security?

Container image security aims to ensure the security of images throughout their lifecycle, including development, deployment, and running. It scans for system vulnerabilities, application vulnerabilities, malicious files, software information, file information, unsafe baseline settings, weak passwords, sensitive information, software compliance issues, and base image information. It helps you identify and fix risks, and ensure images have passed strict checks before being deployed in the production environment, so that your system and applications can run stably and securely.

You can scan CI/CD, repository, and local images in any stage of the container lifecycle.

- **CI/CD images**: During continuous integration (CI) and continuous delivery (CD), you can perform in-depth scans and analysis on container images and eliminate risks before delivery.
- **Repository images**: You can scan for and eliminate risks in the images stored in repositories (such as Harbor and SWR).
- **Local images**: You can scan the container images stored or running on servers to enhance local image security.

Statistics can be presented in the risk view or image view. You can check the risks in a specific image or the images affected by a specific risk. This helps you learn and analyze assets and risks in multiple dimensions, monitoring and managing image risks all in one place.

5.3.2 Enabling Pay-per-use Container Image Scan

Scenarios

To perform the image security scan for repository images and CI/CD images, enable the pay-per-use container image scan.

Billing

- Container image scan is billed per successful image per scan. This function is still in the OBT phase, and its price is displayed on the value-added services sales page. For details about pricing, see **HSS Pricing Details**.
- If you have created scheduled scan tasks for repository images before the pay-per-use container image scan is launched, the tasks will generate costs after you enable the pay-per-use scan. To avoid such costs, disable the scheduled scan policy in advance. For details, see **Periodically Scanning Repository Images**.
- After you enable pay-per-use container image scan, you can scan up to 10 images for free each month. These scans expire at the end of each month.

Method 1: Enable Pay-per-use Scan on the Purchase Page

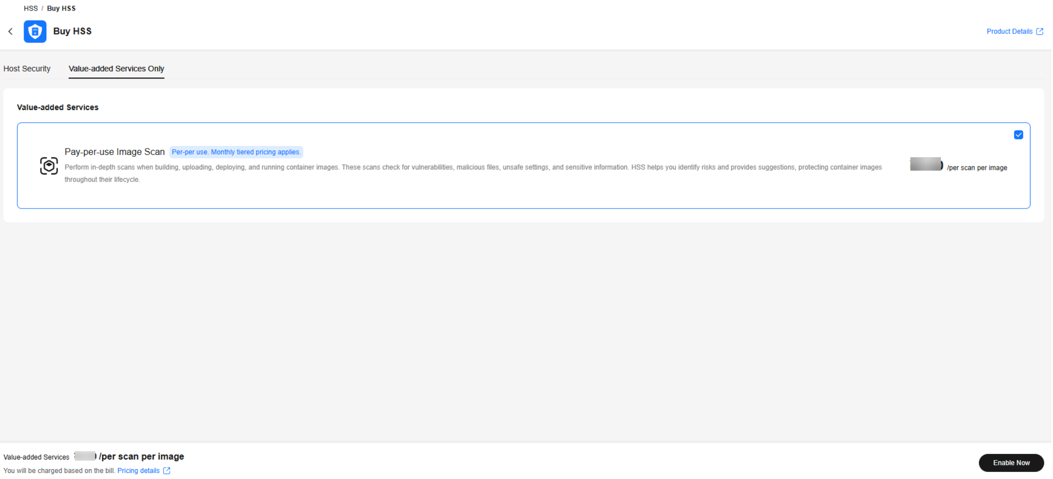
Step 1 **Log in to the management console**.

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

Step 3 In the upper right corner of the **Overview** page, click **Buy HSS**.

Step 4 Click the **Value-added Services Only** tab and select **Pay-per-use Image Scan**.

Figure 5-52 Enabling pay-per-use container image scan



HSS / Buy HSS

Buy HSS

Product Details

Host Security | Value-added Services Only

Value-added Services

☑ Pay-per-use Image Scan Per-per use. Monthly tiered pricing applies.

Perform in-depth scans when building, uploading, deploying, and running container images. These scans check for vulnerabilities, malicious files, unsafe settings, and sensitive information. HSS helps you identify risks and provides suggestions, protecting container images throughout their lifecycle.

[redacted] /per scan per image

Value-added Services [redacted] /per scan per image

You will be charged based on the bill. Pricing details

Enable Now

Step 5 Click **Enable Now** and confirm the order.

----End

Method 2: Enable Pay-per-use Scan on the Container Images Page

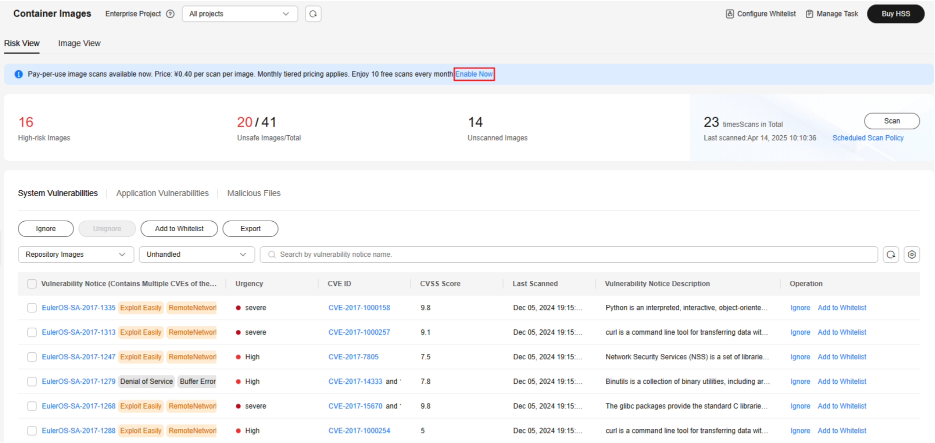
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 Click **Enable Now** next to the billing prompt of the pay-per-use image security scan.

Figure 5-53 Enabling pay-per-use container image scan



Container Images   Enterprise Project   All projects   Configure Whitelist   Manage Task   Buy HSS

Risk View | Image View

Pay-per-use image scans available now. Price: ¥0.40 per scan per image. Monthly tiered pricing applies. Enjoy 10 free scans every month Enable Now

16 High-risk Images

20 / 41 Unsafe Images/Total

14 Unscanned Images

23 timesScans in Total   Scan
Last scanned:Apr 14, 2025 10:10:36   Scheduled Scan Policy

System Vulnerabilities | Application Vulnerabilities | Malicious Files

Ignore   Unignore   Add to Whitelist   Export

Repository Images   Unhandled   Search by vulnerability notice name.

Vulnerability Notice (Contains Multiple CVEs of the...	Urgency	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
EulerOS-SA-2017-1335 Exploit Easily RemoteNetworl	● severe	CVE-2017-1000158	9.8	Dec 05, 2024 19:15:...	Python is an interpreted, interactive, object-oriente...	Ignore Add to Whitelist
EulerOS-SA-2017-1313 Exploit Easily RemoteNetworl	● severe	CVE-2017-1000257	9.1	Dec 05, 2024 19:15:...	curl is a command line tool for transferring data wit...	Ignore Add to Whitelist
EulerOS-SA-2017-1247 Exploit Easily RemoteNetworl	● High	CVE-2017-7805	7.5	Dec 05, 2024 19:15:...	Network Security Services (NSS) is a set of librarie...	Ignore Add to Whitelist
EulerOS-SA-2017-1279 Denial of Service Buffer Error	● High	CVE-2017-14333 and '	7.8	Dec 05, 2024 19:15:...	Binutils is a collection of binary utilities, including ar...	Ignore Add to Whitelist
EulerOS-SA-2017-1268 Exploit Easily RemoteNetworl	● severe	CVE-2017-15670 and '	9.8	Dec 05, 2024 19:15:...	The glibc packages provide the standard C librarie...	Ignore Add to Whitelist
EulerOS-SA-2017-1288 Exploit Easily RemoteNetworl	● High	CVE-2017-1000254	5	Dec 05, 2024 19:15:...	curl is a command line tool for transferring data wit...	Ignore Add to Whitelist

Step 5 After confirming the pay-per-use information, select **I have read and agree to the Host Security Service Disclaimer**.

Step 6 Click **Enable Now** and confirm the order.

----End

Related Operations

Disabling pay-per-use scan

To disable pay-per-use billing, click **Disable Pay-per-use Scan** on the container image page. After it is disabled, you cannot use the free scans you have. All scheduled image scan tasks will be deleted, and historical image scan results will be retained for only 30 days.

5.3.3 CI/CD Image Security Scan

5.3.3.1 CI/CD Image Security Scan Overview

The CI/CD image security scan function of HSS can be integrated into the CI/CD build pipeline of the Jenkins Pipeline project. It can implement security scan in the image build phase; identify system vulnerabilities, application vulnerabilities, unsafe settings, malicious files, sensitive files, and software compliance issues in images; and shift security left to the DevOps phase, helping you eliminate security risks as early as possible and preventing unsafe images from being deployed in the production environment.

What Is CI/CD?

CI/CD is short for continuous integration and continuous delivery/deployment.

- Continuous Integration (CI) automatically and continuously integrates code into shared source code.
- CD consists of continuous delivery and continuous deployment. After continuous integration, continuous delivery verifies the code through automated building and testing to ensure that container images can be delivered at any time. Continuous deployment automatically updates and releases the images to the production environment.

What Is Jenkins Pipeline?

Jenkins is an open source CI tool that provides user-friendly GUIs. It originates from Hudson and is used to automate all sorts of tasks related to building, testing, and delivering or deploying software.

Jenkins is written in Java and can run in popular servlet containers such as Tomcat, or run independently. It is usually used together with the version control tools (or SCM tools) and build tools. Jenkins supports project building in diverse languages and is fully compatible with multiple third-party build tools, such as Maven, Ant, and Gradle. Jenkins is seamlessly integrated with common versioning tools, such as SVN and GIT, and can directly connect to source code hosting websites, such as GitHub.

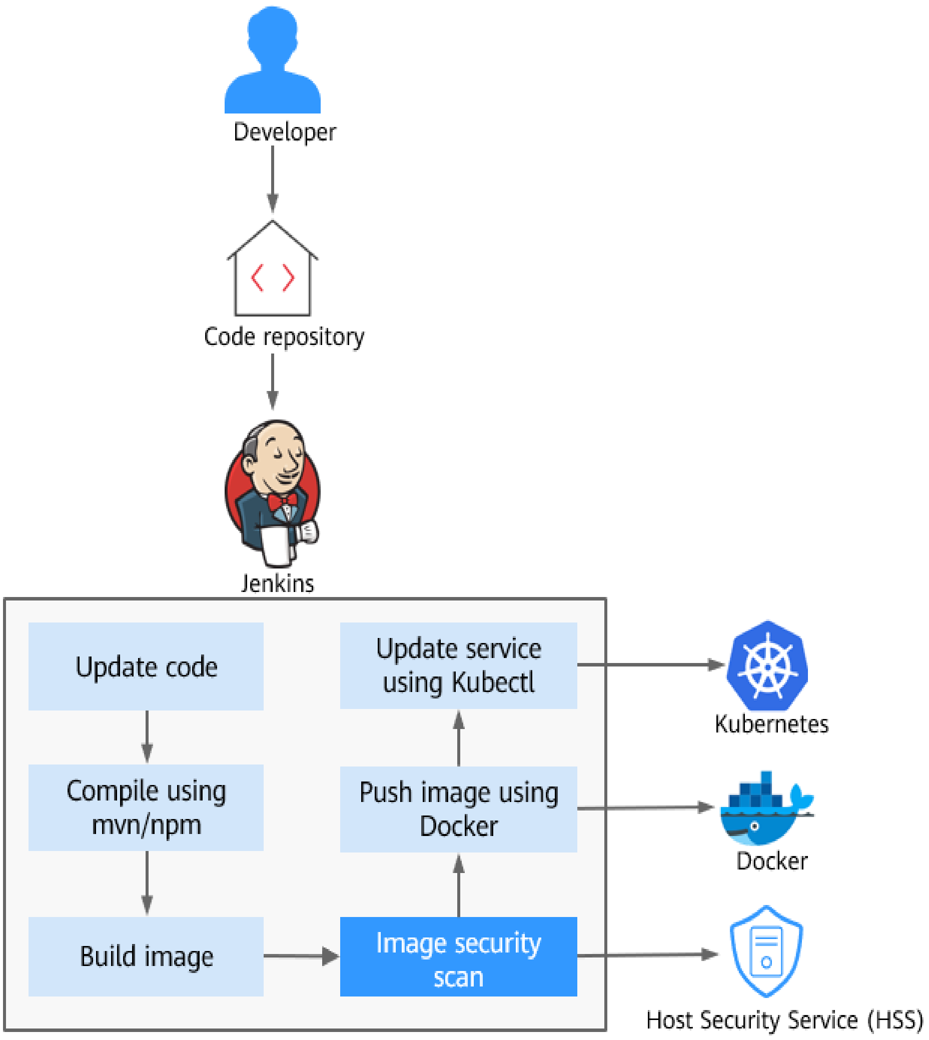
Pipeline is a working mode that implements CI/CD in Jenkins.

CI/CD Image Security Scan Principles

To use the CI/CD image security scan function of HSS, you do not need to synchronize your image assets to HSS. You simply need to add two commands to the Jenkins pipeline (the command for pulling the image of the HSS image security scan tool and the command for starting the tool). When you use Jenkins Pipeline to build a project, an image security scan task is triggered to scan for image security risks in the project and display the scan results on the HSS console. You can handle security risks in images in a timely manner based on the scan results.

Figure 5-54 shows the image security scan phase in the Jenkins pipeline.

Figure 5-54 CI/CD image security scan



CI/CD Image Security Scan Items

Table 5-20 describes the CI/CD image security scan items checked by HSS.

Table 5-20 Image scan items

Scan Item	Description
Vulnerabilities	System and application vulnerabilities in images. ● The following OSs can be scanned: – EulerOS 2.2, 2.3, 2.5, 2.8, 2.9, 2.10, 2.11, 2.12 (64-bit) – CentOS 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 (64-bit) – Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04 (64-bit) – Debian 9, 10, and 11 (64-bit) – Kylin V10, V10 SP1, and V10 SP2 (64-bit) – HCE 1.1 and 2.0 (64-bit) – SUSE 12 SP5, 15 SP1, and 15 SP2 (64-bit) – UnionTech OS V20 server E, V20 server D, 1050u2e, 1050e, 1060e (64-bit) – Rocky Linux 8.4, 8.5, 8.6, 8.10, 9.0, 9.1, 9.2, 9.4, and 9.5 (64-bit) – OpenEuler 20.03, 22.03, and 24.03 (64-bit) – CTyunOS 3-23.01 (64-bit) – AlmaLinux 8.4 (64-bit) ● The following applications and middleware can be scanned: log4j, slf4j, tomcat, apache, jetty, mysql, druid, commons, spring, shiro, struts, struts2, websocket, json, fastjson, xstream, maven, junit, activemq, libintl, ca-certificates-java, httpclient, httpcore, java, javac2, javaee, Apache2, adaptive_server_enterprise, DB2, http_server, Memcached, nginx, PostgreSQL, bootstrap, zookeeper, plexus-utils, and core.
Malicious Files	Malicious files in images.
Software Information	Software information in an image.
File Information	File information in an image.
Baseline Check	● Unsafe configuration: – Images configurations of CentOS 7, Debian 10, EulerOS, and Ubuntu16 – SSH configurations ● Weak passwords of Linux (SSH) accounts ● Password complexity: insecure password complexity policies in Linux

Scan Item	Description
Sensitive Information	Files that contain sensitive information in images. ● The paths that are not checked by default are as follows: – /usr/* – /lib/* – /lib32/* – /bin/* – /sbin/* – /var/lib/* – /var/log/* – *AnyPath*/node_modules/*AnyPath*/*AnyName*.md – *AnyPath*/node_modules/*AnyPath*/test/*AnyPath* – */service/iam/examples_test.go – *AnyPath*/grafana/public/build/*AnyName*.js **NOTE** ● *AnyPath*: indicates that the current path is a customized value and can be any path in the system. ● *AnyName*: indicates that the file name in the current path is a customized value, which can be any name ended with .md or .js in the system. ● On the **View Report** > **Sensitive Information** tab, click **Configure Sensitive File Path** to set the Linux paths of the file that do not need to be checked. A maximum of 20 paths can be added. ● No checks are performed in the following scenarios: – The file size is greater than 20 MB. – The file type is binary, common process, or auto generation.
Software Compliance	Whether software and patch packages contain components that may cause security, compliance, or privacy issues. Examples: ● Third-party network sniffing and debugging tools: tcpdump, gdb, strace, readelf, and Nmap ● Development or compilation tools: Dev-cpp, gcc, and mirror
Base Images	Basic image used for detecting service images.

Scenario

- **Scanning a local image**

  After an image is built, a security scan is performed on it. If the image has security risks, the pipeline can be blocked, so that it will not be pushed to the production image repository.

- **Scanning a remote image repository**

  A remote image repository is a remote test repository pushed after an image is built. A security scan is performed on the image in the remote test repository. If no risks are found, the image can be pushed to the production image repository. If risks are found, the pipeline can be blocked.

Constraints

- To scan repository images, enable pay-per-use container image scans. This feature does not depend on any HSS edition. For details, see **Enabling Pay-per-use Container Image Scan**.
- The CI/CD image scan function applies only to the Jenkins Pipeline mode.

  Jenkins configuration restrictions are as follows:
  - Hardware restrictions:
    - Jenkins compilation and building server: Linux server, x86 or Arm 64-bit
    - CPU: 1 or more cores
    - Memory: 2 GB or more
    - Disk space: 60 GB or higher
  - Technical restrictions:
    - Jenkins version: Jenkins 2.x
    - JDK version: JDK 17 or later
    - Docker version: Docker 18.09 or later
- To perform a remote image scan, the image repository must support interaction through Docker Registry HTTP API v2.

CI/CD Image Security Scan Process

Figure 5-55 Usage process

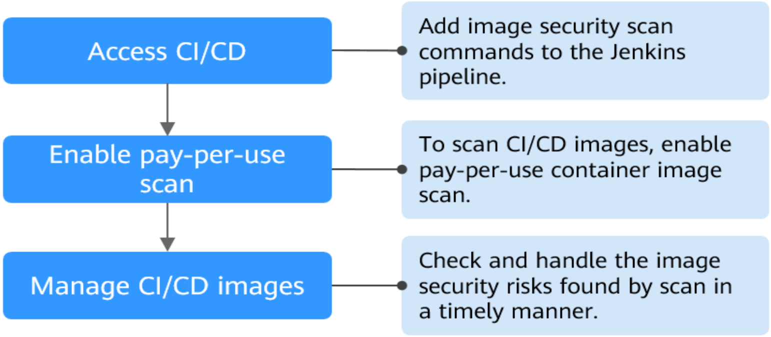

Access CI/CD
Add image security scan commands to the Jenkins pipeline.
Enable pay-per-use scan
To scan CI/CD images, enable pay-per-use container image scan.
Manage CI/CD images
Check and handle the image security risks found by scan in a timely manner.

Table 5-21 Usage process

Operation	Description
Accessing CI/CD	Generate an image security scan command for Pipeline based on image information and add the command to the Jenkins pipeline.
Enabling Pay-per-use Container Image Scan	Enable pay-per-use scan for CI/CD images.
Viewing and Handling CI/CD Image Scan Results	View the CI/CD image security scan results. Check and eliminate security risks to prevent insecure images from entering the production environment.

5.3.3.2 Viewing and Handling CI/CD Image Scan Results

Scenarios

To perform CI/CD image security scans, access CI/CD first. For details, see **Accessing CI/CD**.

After CI/CD is accessed, HSS will check image security during project building in Jenkins Pipeline, and display the scan results on the HSS console. It can help you identify and eliminate image security risks in a timely manner.

HSS can present image security statistics in the risk view and image view, helping you comprehensively learn, locate, and fix image risks.

- Risk view: View all the scan results of a risk, for example, a system vulnerability, application vulnerability, malicious file, unsafe setting, sensitive information risk, or software compliance issue.
- Image view: View the scan results of an image. The results include system vulnerabilities, application vulnerabilities, malicious files, software information, file information, unsafe baseline settings, sensitive information, software compliance, and base image information.

Viewing and Handling CI/CD Image Scan Results in the Risk View

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

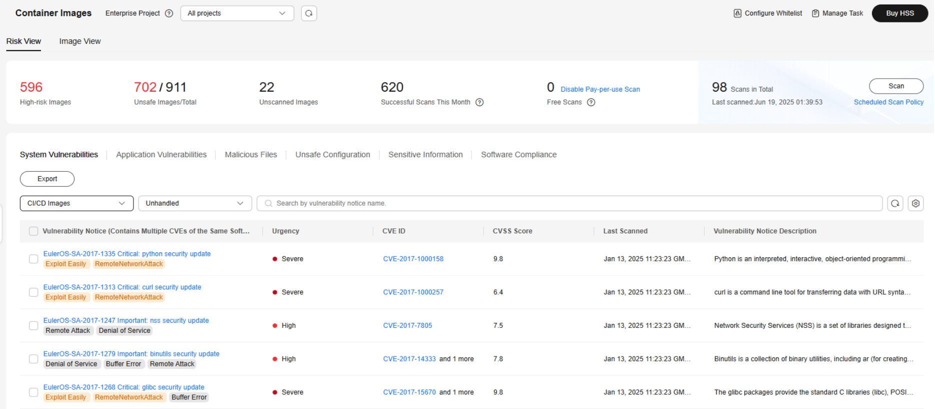
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 On the **Risk View** tab page, click a risk sub-tab, and select **CI/CD Images** from the drop-down list. Check and handle scan results. For details, see **Table 5-22**.

Image names are not displayed for some risks. You can export risk results to obtain these image names and image tags.

Figure 5-56 Risk view of CI/CD images



596 High-risk Images

702 / 911 Unsafe Images/Total

22 Unscanned Images

620 Successful Scans This Month

0 Disable Pay-per-use Scan
Free Scans

98 Scans in Total
Last scanned:Jun 19, 2025 01:39:53

Vulnerability Notice (Contains Multiple CVEs of the Same Soft...	Urgency	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description
EulerOS-SA-2017-1335 Critical: python security update Exploit Easily RemoteNetworkAttack	● Severe	CVE-2017-1000158	9.8	Jan 13, 2025 11:23:23 GM...	Python is an interpreted, interactive, object-oriented programmi...
EulerOS-SA-2017-1313 Critical: curl security update Exploit Easily RemoteNetworkAttack	● Severe	CVE-2017-1000257	6.4	Jan 13, 2025 11:23:23 GM...	curl is a command line tool for transferring data with URL synta...
EulerOS-SA-2017-1247 Important: nss security update Remote Attack Denial of Service	● High	CVE-2017-7805	7.5	Jan 13, 2025 11:23:23 GM...	Network Security Services (NSS) is a set of libraries designed t...
EulerOS-SA-2017-1279 Important: binutils security update Denial of Service Buffer Error Remote Attack	● High	CVE-2017-14333 and 1 more	7.8	Jan 13, 2025 11:23:23 GM...	Binutils is a collection of binary utilities, including ar (for creating...
EulerOS-SA-2017-1268 Critical: glibc security update Exploit Easily RemoteNetworkAttack Buffer Error	● Severe	CVE-2017-15670 and 1 more	9.8	Jan 13, 2025 11:23:23 GM...	The glibc packages provide the standard C libraries (libc), POSI...

Table 5-22 Image scan results

Risk Type	Description
Vulnerability risks (system and application vulnerabilities)	Results of OS and application vulnerability scans. Click a vulnerability notice name to go to the vulnerability details page. You can view the notice details, CVE details (for only system vulnerabilities), suggestions, and affected images. You can fix the vulnerability based on the suggestions.
Malicious Files	Results of malicious image file scans, including the file names, paths, file sizes, image types, affected images, and image tags. You can locate and remove malicious files accordingly.

Risk Type	Description
Unsafe Configuration	Results of image baseline checks, including unsafe settings, password complexity policy risks, and common weak password risks. You can perform operations based on the check type: ● **Unsafe Settings** You can view the check items in the list. In the **Operation** column of a check item, click **View Details**. On the displayed slide-out panel on the right, you can view the audit description, suggestion, and affected images of the check item. ● **Password Complexity Policy Risks** Check **Affected Images** and **Policy Risks**, and modify your password complexity policies based on **Suggestion**. ● **Common Weak Password Risks** The scan result contains the account name, account type, masked weak password, weak password usage duration, affected image, and image tag. You can log in to the account to change its password. To let HSS scan for user-defined weak passwords, perform the following operations: 1. Click **Common Weak Password Detection** and click **Manage Weak Password**. 2. Configure weak passwords and click **OK**.
Sensitive Information	The scan result contains the risk level, file path, sensitive information, rule name (sensitive information type), affected image, and image tag.
Software Compliance	The scan result contains the non-compliant software name, version, path, affected image, and image tag.

----End

Viewing and Handling CI/CD Image Scan Results in the Image View

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

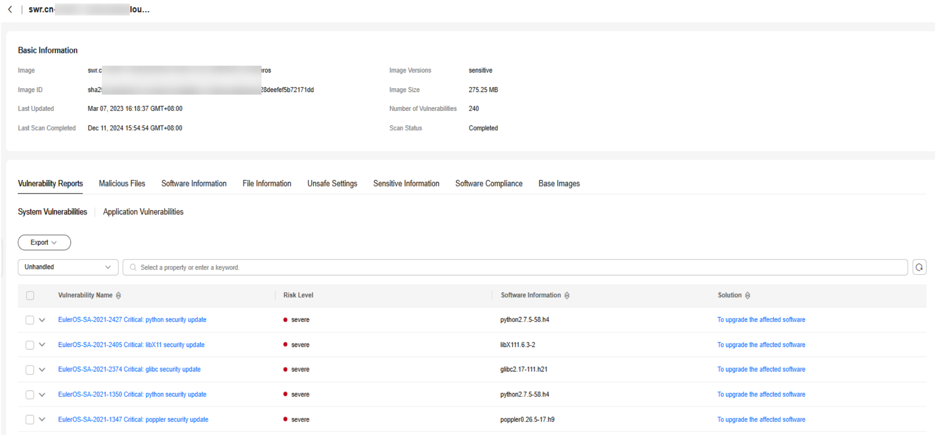
Step 4 Click the **Image View** tab.

Step 5 Click the **CI/CD Images** sub-tab. View CI/CD images.

Step 6 In the **Operation** column of an image, click **View Results** to go to the image details page.

Step 7 View and handle risk scan results. For details, see Table 5-23.

Figure 5-57 CI/CD image scan results



< | swr.cn-[redacted]lou...

Basic Information

Image swr.c[redacted]ros
Image ID sha2[redacted]28deefef5b72171dd
Last Updated Mar 07, 2023 16:18:37 GMT+08:00
Last Scan Completed Dec 11, 2024 15:54:54 GMT+08:00
Image Versions sensitive
Image Size 275.25 MB
Number of Vulnerabilities 240
Scan Status Completed

Vulnerability Reports | Malicious Files | Software Information | File Information | Unsafe Settings | Sensitive Information | Software Compliance | Base Images

System Vulnerabilities | Application Vulnerabilities

Export

Unhandled

Select a property or enter a keyword.

Vulnerability Name	Risk Level	Software Information	Solution
EulerOS-SA-2021-2427 Critical: python security update	● severe	python2.7.5-58.h4	To upgrade the affected software
EulerOS-SA-2021-2405 Critical: libX11 security update	● severe	libX111.6.3-2	To upgrade the affected software
EulerOS-SA-2021-2374 Critical: glibc security update	● severe	glibc2.17-111.h21	To upgrade the affected software
EulerOS-SA-2021-1350 Critical: python security update	● severe	python2.7.5-58.h4	To upgrade the affected software
EulerOS-SA-2021-1347 Critical: poppler security update	● severe	poppler0.26.5-17.h9	To upgrade the affected software

Table 5-23 Image scan results

Risk Type	Description
Vulnerability Reports	Results of OS and application vulnerability scans. - Basic vulnerability information Click a vulnerability name to go to its details page. View the vulnerability description, urgency, and affected images. - Solution – System vulnerabilities Upgrade the software affected by the vulnerability. Click **To upgrade the affected software** to go to the security notice details page. View the affected components, CVE, and more information. – Application vulnerabilities Hover the cursor over the solution description of a vulnerability to view the solution. To install a patch, access the patch installation guide link provided in the solution, and install the patch accordingly.
Malicious Files	Scan results of malicious image files, including the file names, paths, and file sizes. You can locate and remove malicious files accordingly.
Software Information	Statistical results of image software, including the software names, types, versions, and number of software vulnerabilities. Click ⌄ next to a software name to view its vulnerabilities, urgency, and solutions.
File Information	Statistical results of image files, including their file names, paths, and sizes. You can check and remove abnormal files accordingly.

Risk Type	Description
Unsafe Configuration	Results of image baseline checks, including Unsafe Settings, Password Complexity Policy Risks, and Common Weak Password Risks. You can perform operations based on the check type: ● Unsafe Settings You can view the check items in the list. In the **Operation** column of a check item, click **View Details**. On the displayed slide-out panel on the right, you can view the audit description, suggestion, and affected images of the check item. ● Password Complexity Policy Risks Check **Affected Images** and **Policy Risks**, and modify your password complexity policies based on **Suggestion**. ● Common Weak Password Risks The scan result contains the account name, account type, masked weak password, weak password usage duration, affected image, and image tag. You can log in to the account to change its password. To let HSS scan for user-defined weak passwords, perform the following operations: 1. Click **Common Weak Password Detection** and click **Manage Weak Password**. 2. Configure weak passwords and click **OK**.
Sensitive Information	The scan result contains the risk level, file path, content, rule name (sensitive information type), affected image, and image tag.
Software Compliance	The scan result contains the non-compliant software name, version, path, and image tag.
Base Images	Scan results of the base image scan used by a service image. The results include the image name, version, and image layer path.

----End

Related Operations

For details about how to add or modify the vulnerability blacklist, vulnerability whitelist, or image whitelist, see **Editing the Blacklist or Whitelist**.

5.3.3.3 Exporting CI/CD Image Scan Results

Scenarios

Export image scan results to a local PC.

Exporting CI/CD Image Scan Results from the Risk View

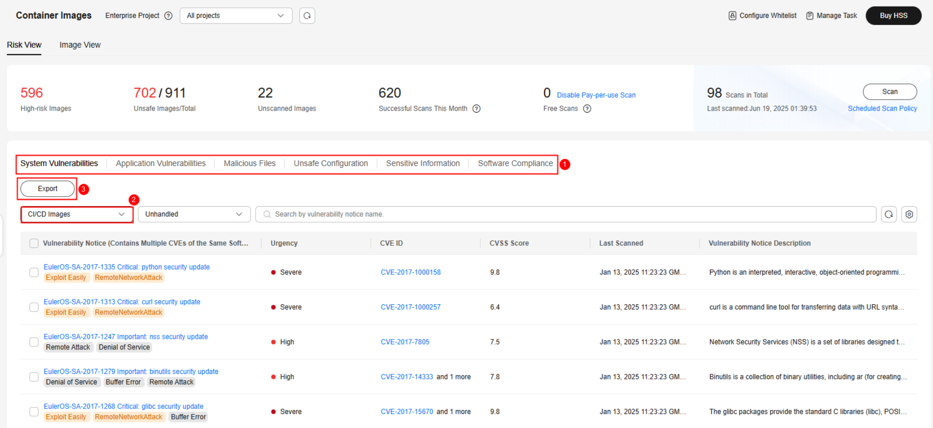
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 On the **Risk View** tab page, click a risk sub-tab, and select **CI/CD Images** from the drop-down list. Click **Export**.

Figure 5-58 Exporting CI/CD image scan results



596 High-risk Images

702 / 911 Unsafe Images/Total

22 Unscanned Images

620 Successful Scans This Month

0 Free Scans

98 Scans in Total

Last scanned:Jun 19, 2025 01:39:53

Vulnerability Notice (Contains Multiple CVEs of the Same Soft...	Urgency	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description
EulerOS-SA-2017-1335 Critical: python security update Exploit Easily RemoteNetworkAttack	Severe	CVE-2017-1000158	9.8	Jan 13, 2025 11:23:23 GM...	Python is an interpreted, interactive, object-oriented programmi...
EulerOS-SA-2017-1313 Critical: curl security update Exploit Easily RemoteNetworkAttack	Severe	CVE-2017-1000257	6.4	Jan 13, 2025 11:23:23 GM...	curl is a command line tool for transferring data with URL synta...
EulerOS-SA-2017-1247 Important: nss security update Remote Attack Denial of Service	High	CVE-2017-7805	7.5	Jan 13, 2025 11:23:23 GM...	Network Security Services (NSS) is a set of libraries designed t...
EulerOS-SA-2017-1279 Important: binutils security update Denial of Service Buffer Error Remote Attack	High	CVE-2017-14333 and 1 more	7.8	Jan 13, 2025 11:23:23 GM...	Binutils is a collection of binary utilities, including ar (for creating...
EulerOS-SA-2017-1268 Critical: glibc security update Exploit Easily RemoteNetworkAttack Buffer Error	Severe	CVE-2017-15670 and 1 more	9.8	Jan 13, 2025 11:23:23 GM...	The glibc packages provide the standard C libraries (libc), POSI...

Step 5 In the displayed dialog box, click **OK**.

Step 6 Wait until an export success message is displayed on the top of the **Container Images** page. Find the exported file in the default download path on your local PC.

Do not close the browser page during the export, or the export will be interrupted.

----End

Exporting CI/CD Image Scan Results from the Image View

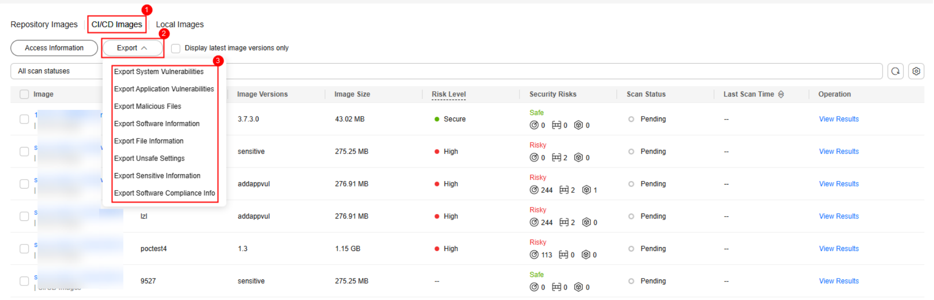
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 On the **Image View** tab page, select **Repository Images**, click **Export**, and choose a risk type.

Figure 5-59 Exporting scan results


1
2
3
Repository Images
CI/CD Images
Local Images
Access Information
Export
□ Display latest image versions only
All scan statuses
Export System Vulnerabilities
Export Application Vulnerabilities
Export Malicious Files
Export Software Information
Export File Information
Export Unsafe Settings
Export Sensitive Information
Export Software Compliance Info

□ Image		Image Versions	Image Size	Risk Level	Security Risks	Scan Status	Last Scan Time	Operation
□ [redacted]		3.7.3.0	43.02 MB	● Secure	Safe 0 0 0	○ Pending	--	View Results
□ [redacted]		sensitive	275.25 MB	● High	Risky 0 2 0	○ Pending	--	View Results
□ [redacted]		addappvul	276.91 MB	● High	Risky 244 2 1	○ Pending	--	View Results
□ [redacted]	lzl	addappvul	276.91 MB	● High	Risky 244 2 0	○ Pending	--	View Results
□ [redacted]	poctest4	1.3	1.15 GB	● High	Risky 113 0 0	○ Pending	--	View Results
□ [redacted]	9527	sensitive	275.25 MB	--	Safe 0 0 0	○ Pending	--	View Results

Step 5 In the displayed dialog box, click **OK**.

Step 6 Wait until an export success message is displayed on the top of the **Container Images** page. Find the exported file in the default download path on your local PC.

Do not close the browser page during the export, or the export will be interrupted.

----End

5.3.4 Repository Image Security Scan

5.3.4.1 Repository Image Security Scan Overview

What Is a Repository Image Security Scan?

The images stored in container image repositories (such as Harbor and SWR) can be shared within or between organizations.

Automatic scans on repository images help you identify and fix vulnerabilities, malware, and other security risks, so that insecure images will not be used in the production environment.

Repository Image Security Scan Principles

HSS can scan images in SWR and third-party repositories.

- **SWR image security scan**

  HSS uses an image scan component to obtain the basic image information and image configuration file (such as the manifest file), and to identify image layers. The layers are downloaded to the HSS cluster and decompressed one by one for scan.

- **Third-party repository image security scan**

  To connect a third-party image repository to HSS for scan, provide the repository information and login credentials, upload the image scan component to the repository, and create a scan task in the repository cluster. HSS obtains the basic image information and configuration file (such as the manifest file) based on the information you provided, and identifies image layers. The layers are downloaded to the repository cluster and decompressed one by one for scan.

Repository Image Security Scan Items

The image security scan items are listed in **Table 5-24**.

Table 5-24 Image scan items

Scan Item	Description
Vulnerabilities	System and application vulnerabilities in images. ● The following OSs can be scanned: – EulerOS 2.2, 2.3, 2.5, 2.8, 2.9, 2.10, 2.11, 2.12 (64-bit) – CentOS 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 (64-bit) – Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04 (64-bit) – Debian 9, 10, and 11 (64-bit) – Kylin V10, V10 SP1, and V10 SP2 (64-bit) – HCE 1.1 and 2.0 (64-bit) – SUSE 12 SP5, 15 SP1, and 15 SP2 (64-bit) – UnionTech OS V20 server E, V20 server D, 1050u2e, 1050e, 1060e (64-bit) – Rocky Linux 8.4, 8.5, 8.6, 8.10, 9.0, 9.1, 9.2, 9.4, and 9.5 (64-bit) – OpenEuler 20.03, 22.03, and 24.03 (64-bit) – CTyunOS 3-23.01 (64-bit) – AlmaLinux 8.4 (64-bit) ● The following applications and middleware can be scanned: log4j, slf4j, tomcat, apache, jetty, mysql, druid, commons, spring, shiro, struts, struts2, websocket, json, fastjson, xstream, maven, junit, activemq, libintl, ca-certificates-java, httpclient, httpcore, java, javac2, javaee, Apache2, adaptive_server_enterprise, DB2, http_server, Memcached, nginx, PostgreSQL, bootstrap, zookeeper, plexus-utils, and core.
Malicious Files	Malicious files in images.
Software Information	Software information in an image.
File Information	File information in an image.
Baseline Check	● Unsafe configuration: – Images configurations of CentOS 7, Debian 10, EulerOS, and Ubuntu16 – SSH configurations ● Weak passwords of Linux (SSH) accounts ● Password complexity: insecure password complexity policies in Linux

Scan Item	Description
Sensitive Information	Files that contain sensitive information in images. ● The paths that are not checked by default are as follows: – /usr/* – /lib/* – /lib32/* – /bin/* – /sbin/* – /var/lib/* – /var/log/* – *AnyPath*/node_modules/*AnyPath*/*AnyName*.md – *AnyPath*/node_modules/*AnyPath*/test/*AnyPath* – */service/iam/examples_test.go – *AnyPath*/grafana/public/build/*AnyName*.js **NOTE** ● *AnyPath*: indicates that the current path is a customized value and can be any path in the system. ● *AnyName*: indicates that the file name in the current path is a customized value, which can be any name ended with .md or .js in the system. ● On the **View Report** > **Sensitive Information** tab, click **Configure Sensitive File Path** to set the Linux paths of the file that do not need to be checked. A maximum of 20 paths can be added. ● No checks are performed in the following scenarios: – The file size is greater than 20 MB. – The file type is binary, common process, or auto generation.
Software Compliance	Whether software and patch packages contain components that may cause security, compliance, or privacy issues. Examples: ● Third-party network sniffing and debugging tools: tcpdump, gdb, strace, readelf, and Nmap ● Development or compilation tools: Dev-cpp, gcc, and mirror
Base Images	Basic image used for detecting service images.

Scenarios

- **Scan images across clouds.**

  In multi-cloud scenarios, security tools or solutions may vary depending on cloud platforms, making it difficult to enhance security in a unified manner. Our scans can check repository images both inside and outside the cloud. You can perform scans and apply unified security policies across clouds, reducing O&M costs.

- **Prevent unsafe images from entering the production environment.**

  Before images are deployed in the production environment, scan for and fix vulnerabilities and malicious files to ensure image security upon deployment.

Constraints

- To scan repository images, enable pay-per-use container image scans. This feature does not depend on any HSS edition. For details, see **Enabling Pay-per-use Container Image Scan**.
- Only Linux images can be scanned.
- Prerequisites for scanning a third-party image repository:
  a. The repository cluster (cluster where the repository is deployed) has been connected to HSS and is in the **Running** state. For details, see **Overview of Agent Installation in a Cluster**.

     You can connect to the following third-party cloud cluster service providers: Alibaba Cloud, Tencent Cloud, AWS, Microsoft Azure, user-built clouds, and user-built IDCs.

  b. The third-party image repository has been connected to HSS. For details, see **Connecting to a Third-party Image Repository**.

     Harbor and JFrog image repositories are supported.

Repository Image Security Scan Process

Figure 5-60 Usage process

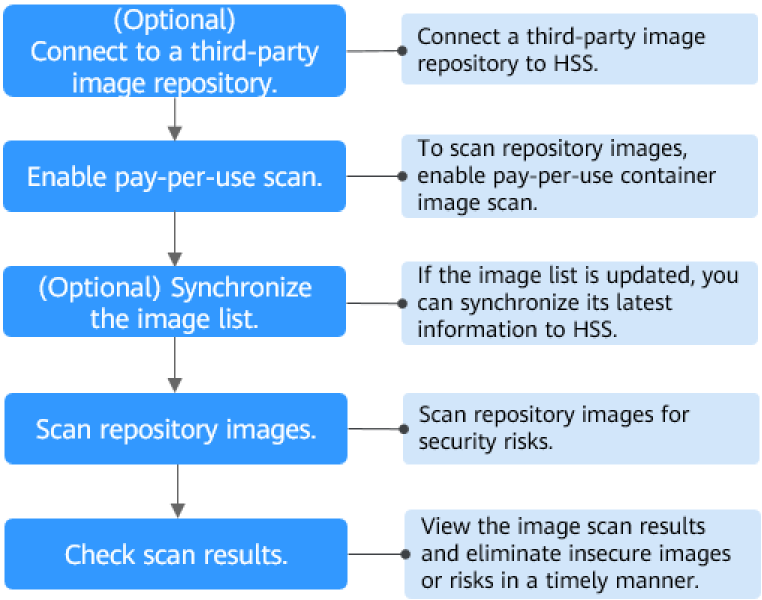

(Optional) Connect to a third-party image repository.
Connect a third-party image repository to HSS.
Enable pay-per-use scan.
To scan repository images, enable pay-per-use container image scan.
(Optional) Synchronize the image list.
If the image list is updated, you can synchronize its latest information to HSS.
Scan repository images.
Scan repository images for security risks.
Check scan results.
View the image scan results and eliminate insecure images or risks in a timely manner.

Table 5-25 Process description

Operation	Description
Connecting to a Third-party Image Repository	You can connect Harbor and JFrog repositories to HSS to scan for and handle their image risks.
Enabling Pay-per-use Container Image Scan	Enable pay-per-use scan for repository images.
(Optional) **Synchronizing Repository Images**	If the image list of your repository is updated, you can synchronize the latest image list to HSS.
Scanning Repository Images	Perform a manual scan or configure a scheduled scan to identify risks in repository images.
Viewing and Handling Repository Image Scan Results	View the repository image security scan results. Check and eliminate security risks to prevent insecure images from entering the production environment.

5.3.4.2 Synchronizing Repository Images

Scenarios

If the information about your repository images changes, you can use either of the following methods to synchronize the image list:

- Manual synchronization: Start an image synchronization task to synchronize the image list. For details, see **Manually Synchronizing Repository Images**.
- Scheduled synchronization: Grant the **SWROperatePolicy** and **CCEOperatePolicy** permissions to HSS. It will automatically synchronize the image list at 01:00 every day by default. If the required permissions are not granted, the synchronization task will fail. For details, see **Authorization**.

Only the basic information about repository images will be synchronized. This operation will neither download SWR images to HSS nor download third-party repository images to any jumper cluster.

Constraints

SWR image synchronization depends on SWR authorization. For details, see **SWR Authorization Methods**.

Manually Synchronizing Repository Images

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 Click the **Image View** tab.

Figure 5-61 Image view

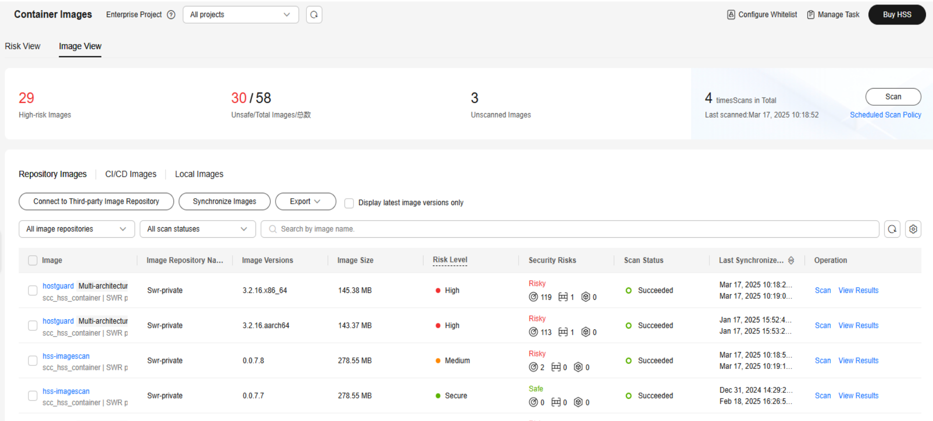
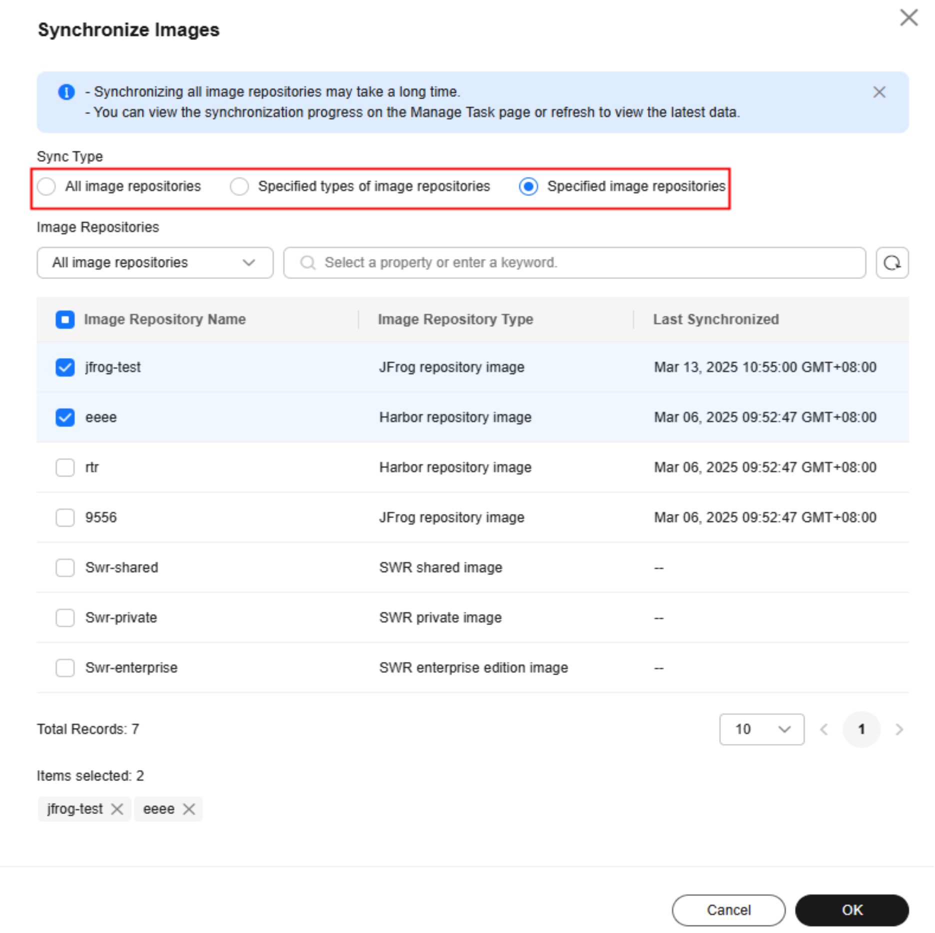


Image	Image Repository Na...	Image Versions	Image Size	Risk Level	Security Risks	Scan Status	Last Synchronize...	Operation
hostguard Multi-architectur scc_hss_container | SWR p	Swr-private	3.2.16.x86_64	145.38 MB	● High	Risky 119 1 0	Succeeded	Mar 17, 2025 10:18:2... Mar 17, 2025 10:19:0...	Scan View Results
hostguard Multi-architectur scc_hss_container | SWR p	Swr-private	3.2.16.aarch64	143.37 MB	● High	Risky 113 1 0	Succeeded	Jan 17, 2025 15:52:4... Jan 17, 2025 15:53:2...	Scan View Results
hss-imagescan scc_hss_container | SWR p	Swr-private	0.0.7.8	278.55 MB	● Medium	Risky 2 0 0	Succeeded	Mar 17, 2025 10:18:5... Mar 17, 2025 10:19:1...	Scan View Results
hss-imagescan scc_hss_container | SWR p	Swr-private	0.0.7.7	278.55 MB	● Secure	Safe 0 0 0	Succeeded	Dec 31, 2024 14:29:2... Feb 18, 2025 16:26:5...	Scan View Results

Step 5 Click **Synchronize Images**.

Step 6 In the **Synchronize Images** slide-out panel, select a synchronization type.

Figure 5-62 Synchronizing images



Synchronize Images

- Synchronizing all image repositories may take a long time.
- You can view the synchronization progress on the Manage Task page or refresh to view the latest data.

Sync Type

○ All image repositories ○ Specified types of image repositories ● Specified image repositories

Image Repositories

All image repositories | Select a property or enter a keyword.

☑ Image Repository Name	Image Repository Type	Last Synchronized
☑ jfrog-test	JFrog repository image	Mar 13, 2025 10:55:00 GMT+08:00
☑ eeee	Harbor repository image	Mar 06, 2025 09:52:47 GMT+08:00
□ rtr	Harbor repository image	Mar 06, 2025 09:52:47 GMT+08:00
□ 9556	JFrog repository image	Mar 06, 2025 09:52:47 GMT+08:00
□ Swr-shared	SWR shared image	--
□ Swr-private	SWR private image	--
□ Swr-enterprise	SWR enterprise edition image	--

Total Records: 7

Items selected: 2

jfrog-test × eeee ×

Table 5-26 Synchronization types

Type	Description
All image repositories	SWR private images, SWR shared images, SWR enterprise images, Harbor images, and JFrog images.
Specified types of image repositories	In the displayed drop-down list, select the types of repository images to be synchronized. ● **SWR private image** ● **SWR shared image** ● **SWR enterprise edition image** ● **Harbor repository image** ● **JFrog repository image**
Specified image repositories	Filter repositories by type or other conditions, and select repositories.

Step 7 Confirm the synchronization type and click **OK**.

Step 8 In the upper right corner of the page, click **Manage Task**. On the **Image Synchronization** tab page, view the synchronization status.

----End

5.3.4.3 Scanning Repository Images

Scenarios

Repository images can be scanned manually or periodically.

- Manual scan: Scan one or multiple images to learn their security status in real time.
- Scheduled scan: Configure a scheduled scan policy to periodically check for image risks. In this mode, only third-party repository images, such as Harbor and Jfrog, can be scanned.

Prerequisites

- You have enabled the **pay-per-use container image scan**. You will be paid per image per scan. For details, see **Enabling Pay-per-use Container Image Scan**.
- You have connected your third-party image repositories (if any) to HSS. For details, see **Connecting to a Third-party Image Repository**.

Constraints

- SWR shared images can be scanned only if they are valid.
- Multi-architecture images do not support manual or scheduled scan.

Manually Scanning Repository Images

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

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

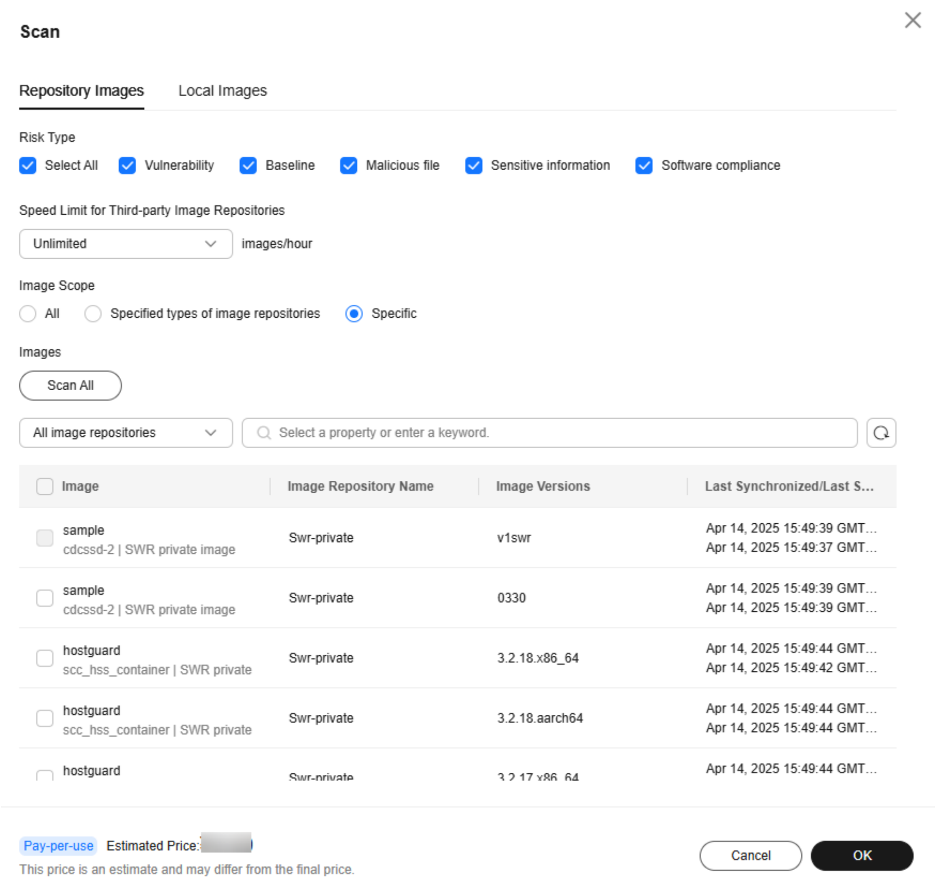
Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In the upper right part of the page, click **Scan**.

To scan a single image, you can also click the **Image View** tab, click **Scan** in the **Operation** column of the image.

Step 5 Click the **Repository Images** tab and configure parameters. For details, see **Table 5-27**.

Figure 5-63 Manually scanning repository images



Scan

Repository Images | Local Images

Risk Type

☑ Select All ☑ Vulnerability ☑ Baseline ☑ Malicious file ☑ Sensitive information ☑ Software compliance

Speed Limit for Third-party Image Repositories

Unlimited images/hour

Image Scope

○ All ○ Specified types of image repositories ● Specific

Images

Scan All

All image repositories | Select a property or enter a keyword.

□ Image	Image Repository Name	Image Versions	Last Synchronized/Last S...
□ sample cdcssd-2 | SWR private image	Swr-private	v1swr	Apr 14, 2025 15:49:39 GMT... Apr 14, 2025 15:49:37 GMT...
□ sample cdcssd-2 | SWR private image	Swr-private	0330	Apr 14, 2025 15:49:39 GMT... Apr 14, 2025 15:49:39 GMT...
□ hostguard scc_hss_container | SWR private	Swr-private	3.2.18.x86_64	Apr 14, 2025 15:49:44 GMT... Apr 14, 2025 15:49:42 GMT...
□ hostguard scc_hss_container | SWR private	Swr-private	3.2.18.aarch64	Apr 14, 2025 15:49:44 GMT... Apr 14, 2025 15:49:44 GMT...
□ hostguard	Swr-private	3.2.17.x86_64	Apr 14, 2025 15:49:44 GMT...

Pay-per-use Estimated Price: [redacted]

This price is an estimate and may differ from the final price.

Cancel OK

Table 5-27 Manual scan parameters

Parameter	Description	Example Value
Risk Type	Select the risk types to be scanned for. Options are **Vulnerability risk**, **Baseline**, **Malicious file**, **Sensitive information**, and **Software compliance**. HSS scans for software information, file information, and base images by default.	All
Speed Limit for Third-party Image Repositories	If you have many third-party images to scan, but do not want the scan to occupy too much bandwidth, you can click ⌄ to set the number of images to be scanned per hour.	Unlimited
Image Scope	Select **All**, **Specified types of image repositories**, or **Specific**. A full scan takes a long time and cannot be stopped once started. Exercise caution when performing this operation.	All

Step 6 Confirm the fees and click **OK** to start the scan.

Step 7 In the upper right corner of the page, click **Manage Task** Click the **Image Scan** tab to view the scan status.

Step 8 After the image scan task is complete, return to **Image View**. You can view the scan status of each image. For details, see **Table 5-28**.

Table 5-28 Risk status

Status	Description
Pending	The image is not scanned.
Scanning	The image is being scanned.
Succeeded	The image has been scanned. You can view the scan results.
Failed	An error or problem occurred during image scan. As a result, the scan failed.
To be scanned	A scan task has been created, and the image is waiting to be scanned.
Scan terminated	The scan task has been canceled, and the image scan has been stopped.

----End

Periodically Scanning Repository Images

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

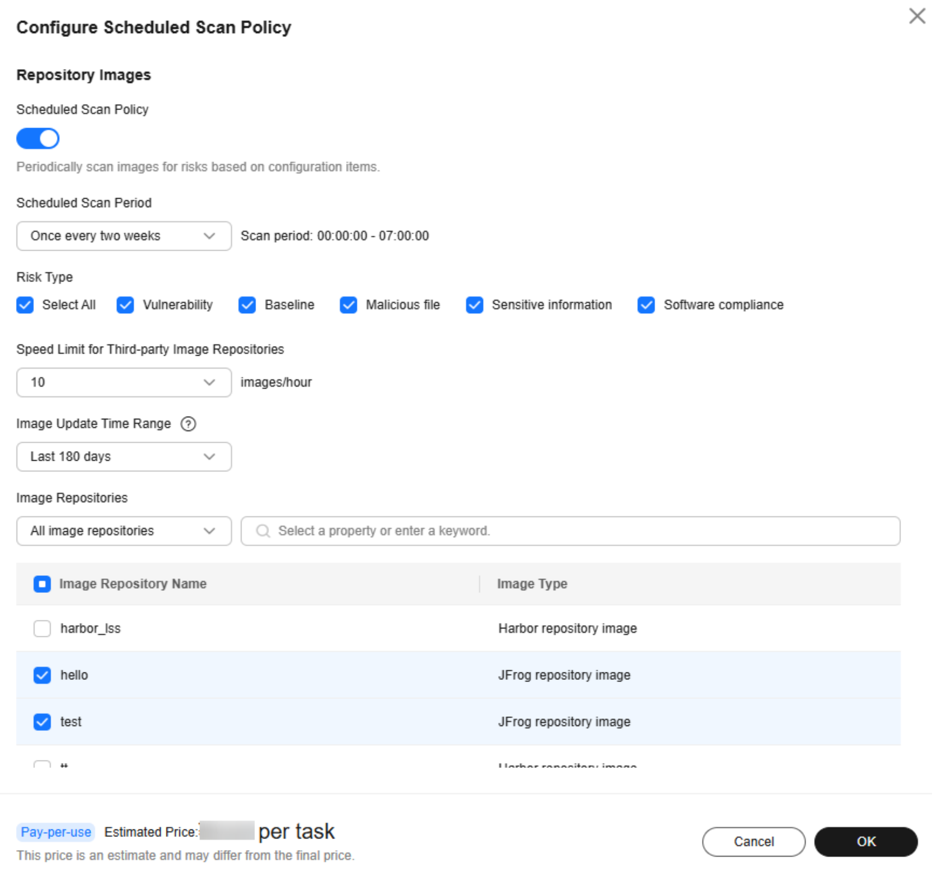
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In the upper right part of the page, click **Scheduled Scan Policy**.

Step 5 Configure scheduled scan parameters, as shown in **Figure 5-64**. For details, see **Table 5-29**.

Figure 5-64 Scheduled scan policy



Configure Scheduled Scan Policy

Repository Images

Scheduled Scan Policy

Periodically scan images for risks based on configuration items.

Scheduled Scan Period

Once every two weeks — Scan period: 00:00:00 - 07:00:00

Risk Type

☑ Select All ☑ Vulnerability ☑ Baseline ☑ Malicious file ☑ Sensitive information ☑ Software compliance

Speed Limit for Third-party Image Repositories

10 images/hour

Image Update Time Range

Last 180 days

Image Repositories

All image repositories — Select a property or enter a keyword.

	Image Repository Name	Image Type
□	harbor_lss	Harbor repository image
☑	hello	JFrog repository image
☑	test	JFrog repository image

Pay-per-use Estimated Price:[redacted] per task

This price is an estimate and may differ from the final price.

Table 5-29 Scheduled scan parameters

Parameter	Description	Example Value
Scheduled Scan Policy	Whether to enable scheduled scan. After this function is enabled, you can view and configure scheduled scan parameters. • ○: disabled • ●: enabled	●
Scheduled Scan Period	Click ⌄ to set the scan period. The scan time range is fixed to 00:00:00 - 07:00:00.	Every 3 days
Risk Type	Select the risk types to be scanned for. Options are **Vulnerability risk**, **Baseline**, **Malicious file**, **Sensitive information**, and **Software compliance**. HSS scans for software information, file information, and base images by default.	All

Parameter	Description	Example Value
Speed Limit for Third-party Image Repositories	If you have many images to scan, but do not want the scan to occupy too much bandwidth, click ⌄ to set the number of images to be scanned per hour.	Unlimited
Image Update Time Range	Select a range of image update time. It determines which images will be scanned. For example, if **Last 15 days** is selected, HSS will only scan the images updated in the last 15 days.	Last 15 days
Image Repositories	Select image repositories.	Harbor repository image

Step 6 Confirm the fees and click **OK** to start the scan.

Step 7 In the upper right corner of the page, click **Manage Task** Click the **Image Scan** tab to view the scan status.

Step 8 After the image scan task is complete, return to **Image View**. You can view the scan status of each image. For details, see **Table 5-30**.

Table 5-30 Risk status

Status	Description
Pending	The image is not scanned.
Scanning	The image is being scanned.
Succeeded	The image has been scanned. You can view the scan results.
Failed	An error or problem occurred during image scan. As a result, the scan failed.
To be scanned	A scan task has been created, and the image is waiting to be scanned.
Scan terminated	The scan task has been canceled, and the image scan has been stopped.

----End

Stopping a Scan Task

You can stop a running scan task.

Constraints

The following permissions are required for IAM users to stop a scan:

- HSS permission: batch image scan (hss:images:set) or container asset management (hss:containers:set) For details, see **Using IAM to Grant Access to HSS**.
- Namespace permission (Kubernetes RBAC): the permission for deleting **job** or **cronjob** resources in HSS namespaces

Procedure

Step 1 In the upper right corner of the **Container Images** page, click **Manage Task**.

Step 2 Click the **Image Scan** tab.

Step 3 In the **Operation** column of a task, click **Cancel Scan**.

Step 4 If **Cancelled** is displayed in the **Scan Status** column of the task, the scan has been canceled.

----End

5.3.4.4 Viewing and Handling Repository Image Scan Results

Scenarios

HSS can present image security statistics in the risk view and image view, helping you comprehensively learn, locate, and fix image risks.

- Risk view: View all the scan results of a risk, for example, a system vulnerability, application vulnerability, malicious file, unsafe setting, sensitive information risk, or software compliance issue.
- Image view: View the scan results of an image. The results include system vulnerabilities, application vulnerabilities, malicious files, software information, file information, unsafe baseline settings, sensitive information, software compliance, and base image information.

You can view and handle repository image scan results in **Risk View** or **Image View**.

Viewing and Handling Repository Image Scan Results in the Risk View

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

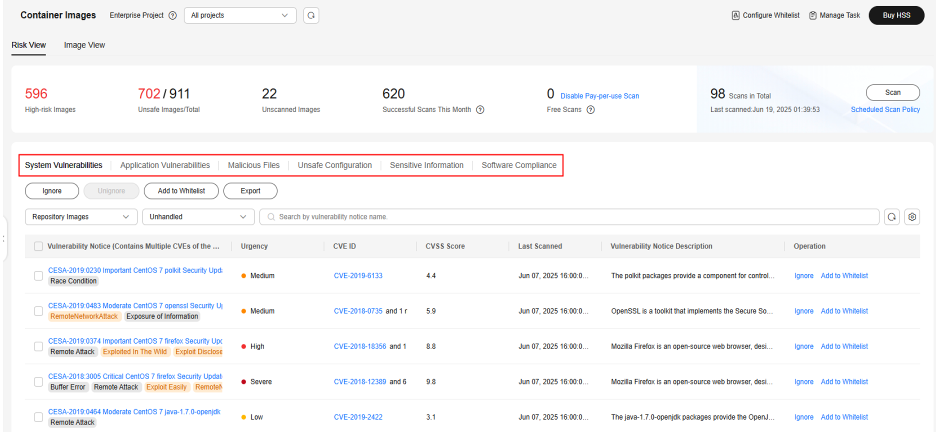
Step 2 In the upper left corner of the page, select a region, click ≡, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 Click the **Risk View** tab. Click a risk sub-tab, and select **Repository Images** from the drop-down list. Check and handle scan results. For details, see **Table 5-31**.

Image names are not displayed for some risks. You can export risk results to obtain these image names and image tags.

Figure 5-65 Repository image risk view



Vulnerability Notice (Contains Multiple CVEs of the ...	Urgency	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
CESA-2019:0230 Important CentOS 7 polkit Security Upd Race Condition	● Medium	CVE-2019-6133	4.4	Jun 07, 2025 16:00:0...	The polkit packages provide a component for control...	Ignore Add to Whitelist
CESA-2019:0483 Moderate CentOS 7 openssl Security U RemoteNetworkAttack Exposure of Information	● Medium	CVE-2018-0735 and 1 r	5.9	Jun 07, 2025 16:00:0...	OpenSSL is a toolkit that implements the Secure So...	Ignore Add to Whitelist
CESA-2019:0374 Important CentOS 7 firefox Security Upc Remote Attack Exploited In The Wild Exploit Disclose	● High	CVE-2018-18356 and 1	8.8	Jun 07, 2025 16:00:0...	Mozilla Firefox is an open-source web browser, desi...	Ignore Add to Whitelist
CESA-2018:3005 Critical CentOS 7 firefox Security Updat Buffer Error Remote Attack Exploit Easily RemoteN	● Severe	CVE-2018-12389 and 6	9.8	Jun 07, 2025 16:00:0...	Mozilla Firefox is an open-source web browser, desi...	Ignore Add to Whitelist
CESA-2019:0464 Moderate CentOS 7 java-1.7.0-openjdk Remote Attack	● Low	CVE-2019-2422	3.1	Jun 07, 2025 16:00:0...	The java-1.7.0-openjdk packages provide the OpenJ...	Ignore Add to Whitelist

Table 5-31 Image scan results

Risk Type	Description
Vulnerability Reports (system and application vulnerabilities)	Results of OS and application vulnerability scans. You can: ● View vulnerability details Click a vulnerability name. On the vulnerability details page, view the vulnerability notice, CVE (for system vulnerabilities only), suggestions, affected images, and handling history. ● Handle vulnerabilities – Ignore If a vulnerability does not need to be handled for now, you can ignore it. It will still be displayed in future scan results. – Add to whitelist If a vulnerability does not affect your services, you can add it to the whitelist. – Fix Fix the vulnerability by referring to the suggestions in the vulnerability details.
Malicious Files	Detected malicious image files. Their file names, paths, and sizes are displayed. You can locate and remove malicious files accordingly.

Risk Type	Description
Unsafe Configuration	Image baseline check result, including Unsafe Settings, Password Complexity Policy Risks, and Common Weak Password Risks. You can perform operations based on the check type: ● Unsafe Settings You can view the check items in the list. In the **Operation** column of a check item, click **View Details**. On the displayed slide-out panel on the right, you can view the audit description, suggestion, and affected images of the check item. ● Password Complexity Policy Risks Check **Affected Images** and **Policy Risks**, and modify your password complexity policies based on **Suggestion**. ● Common Weak Password Risks The scan result contains the account name, account type, masked weak password, weak password usage duration, affected image, and image tag. You can log in to the account to change its password. To let HSS scan for user-defined weak passwords, perform the following operations: 1. Click the **Common Weak Password Risks** tab and click **Manage Weak Password**. 2. Configure weak passwords and click **OK**.
Sensitive Information	The scan result contains the risk level, file path, sensitive information, rule name (sensitive information type), affected image, and image tag.
Software Compliance	The scan result contains the non-compliant software name, version, path, affected image, and image tag.

----End

Viewing and Handling Repository Image Scan Results in the Image View

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

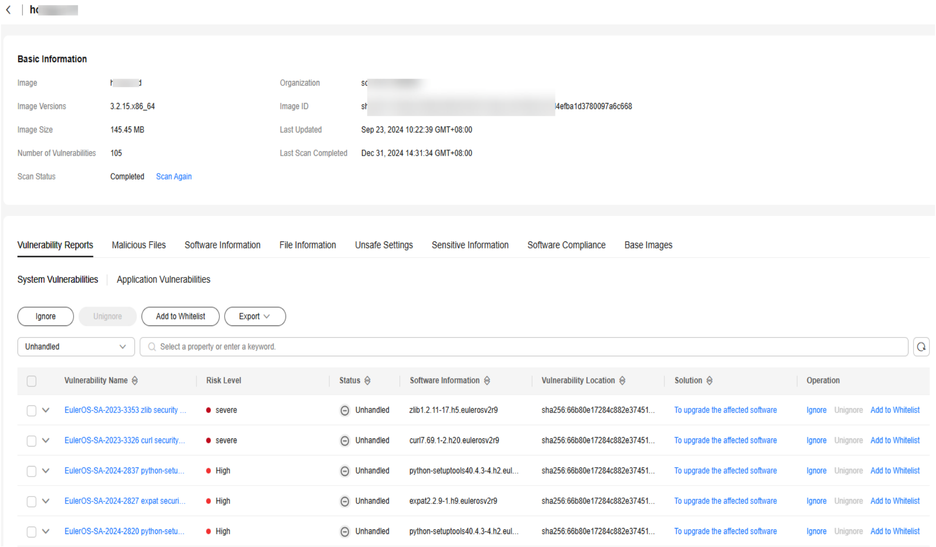
Step 4 Click the **Image View** tab.

Step 5 Click the **Repository Images** tab.

Step 6 In the **Operation** column of an image, click **View Results** to go to the image details page.

Step 7 View and handle risk scan results. For details, see **Table 5-32**.

Figure 5-66 Repository image scan details



[redacted]

Basic Information

Image	[redacted]	Organization	[redacted]
Image Versions	3.2.15.x86_64	Image ID	sh[redacted]4efba1d3780097a6c668
Image Size	145.45 MB	Last Updated	Sep 23, 2024 10:22:39 GMT+08:00
Number of Vulnerabilities	105	Last Scan Completed	Dec 31, 2024 14:31:34 GMT+08:00
Scan Status	Completed Scan Again		

□	Vulnerability Name	Risk Level	Status	Software Information	Vulnerability Location	Solution	Operation
□	EulerOS-SA-2023-3353 zlib security ...	● severe	Unhandled	zlib1.2.11-17.h5.eulerosv2r9	sha256:66b80e17284c882e37451...	To upgrade the affected software	Ignore Unignore Add to Whitelist
□	EulerOS-SA-2023-3326 curl security...	● severe	Unhandled	curl7.69.1-2.h20.eulerosv2r9	sha256:66b80e17284c882e37451...	To upgrade the affected software	Ignore Unignore Add to Whitelist
□	EulerOS-SA-2024-2837 python-setu...	● High	Unhandled	python-setuptools40.4.3-4.h2.eul...	sha256:66b80e17284c882e37451...	To upgrade the affected software	Ignore Unignore Add to Whitelist
□	EulerOS-SA-2024-2827 expat securi...	● High	Unhandled	expat2.2.9-1.h9.eulerosv2r9	sha256:66b80e17284c882e37451...	To upgrade the affected software	Ignore Unignore Add to Whitelist
□	EulerOS-SA-2024-2820 python-setu...	● High	Unhandled	python-setuptools40.4.3-4.h2.eul...	sha256:66b80e17284c882e37451...	To upgrade the affected software	Ignore Unignore Add to Whitelist

Table 5-32 Image scan result parameters

Risk Type	Description
Vulnerability Reports	Results of OS and application vulnerability scans. You can: ● View vulnerability details Click a vulnerability name to go to its details page. View the vulnerability description, urgency, and affected images. ● Handle vulnerabilities – Ignore If a vulnerability does not need to be handled for now, you can ignore it. It will still be displayed in future scan results. – Add to whitelist If a vulnerability does not affect your services, you can add it to the whitelist. – Fix To fix a system vulnerability, upgrade the software affected by it. Click **To upgrade the affected software** to go to the security notice details page. View the affected components, CVE, and more information. To fix an application vulnerability, hover the cursor over the solution description of a vulnerability to view the solution. To install a patch, access the patch installation guide link provided in the solution, and install the patch accordingly.
Malicious Files	Scan results of malicious image files, including the file names, paths, and file sizes. You can locate and remove malicious files accordingly.

Risk Type	Description
Software Information	Statistical results of image software, including the software names, types, versions, and number of software vulnerabilities. Click ⌄ next to a software name to view its vulnerability name, urgency, and solution.
File Information	Statistical results of image files, including their file names, paths, and sizes. You can check and remove abnormal files accordingly.
Unsafe Configuration	Image baseline check result, including Unsafe Settings, Password Complexity Policy Risks, and Common Weak Password Risks. You can perform operations based on the check type: ● Unsafe Settings You can view the check items in the list. In the **Operation** column of a check item, click **View Details**. On the displayed slide-out panel on the right, you can view the audit description, suggestion, and affected images of the check item. ● Password Complexity Policy Risks Check **Affected Images** and **Policy Risks**, and modify your password complexity policies based on **Suggestion**. ● Common Weak Password Risks The scan result contains the account name, account type, masked weak password, weak password usage duration, affected image, and image tag. You can log in to the account to change its password. To let HSS scan for user-defined weak passwords, perform the following operations: 1. Click the **Common Weak Password Detection** tab and click **Manage Weak Password**. 2. Configure weak passwords and click **OK**.
Sensitive Information	The scan result contains the risk level, file path, content, rule name (sensitive information type), affected image, and image tag.
Software Compliance	The scan result contains the non-compliant software name, version, path, and image tag.
Base Images	Scan results of the base image scan used by a service image. The results include the image name, version, and image layer path.

----End

5.3.4.5 Exporting Repository Image Scan Results

Scenarios

Export image scan results to a local PC.

Exporting Repository Image Scan Results from the Risk View

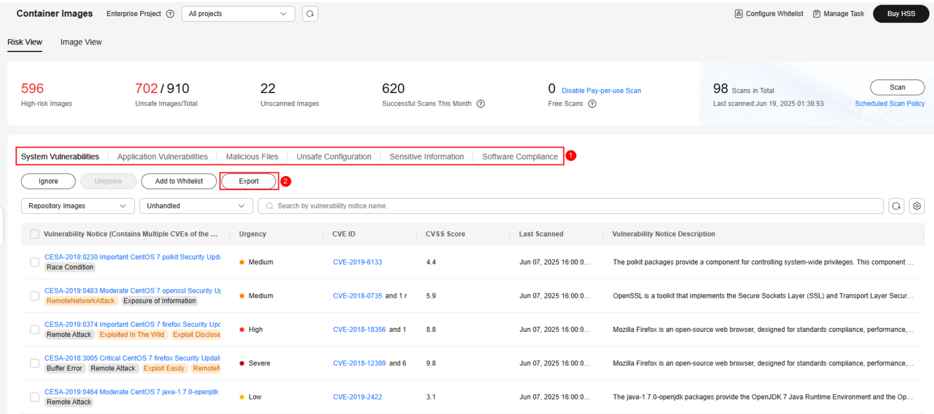
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 On the **Risk View** tab page, select risks and click **Export**.

Figure 5-67 Exporting scan results



Vulnerability Notice (Contains Multiple CVEs of the ...	Urgency	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description
CESA-2019:0230 Important CentOS 7 polkit Security Upd Race Condition	● Medium	CVE-2019-6133	4.4	Jun 07, 2025 16:00:0...	The polkit packages provide a component for controlling system-wide privileges. This component ...
CESA-2019:0483 Moderate CentOS 7 openssl Security U RemoteNetworkAttack Exposure of Information	● Medium	CVE-2018-0735 and 1 r	5.9	Jun 07, 2025 16:00:0...	OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Secur...
CESA-2019:0374 Important CentOS 7 firefox Security Upc Remote Attack Exploited In The Wild Exploit Disclose	● High	CVE-2018-18356 and 1	8.8	Jun 07, 2025 16:00:0...	Mozilla Firefox is an open-source web browser, designed for standards compliance, performance,...
CESA-2018:3005 Critical CentOS 7 firefox Security Updat Buffer Error Remote Attack Exploit Easily Remote	● Severe	CVE-2018-12389 and 6	9.8	Jun 07, 2025 16:00:0...	Mozilla Firefox is an open-source web browser, designed for standards compliance, performance,...
CESA-2019:0464 Moderate CentOS 7 java-1.7.0-openjdk Remote Attack	● Low	CVE-2019-2422	3.1	Jun 07, 2025 16:00:0...	The java-1.7.0-openjdk packages provide the OpenJDK 7 Java Runtime Environment and the Op...

Step 5 In the displayed dialog box, click **OK**.

Step 6 Wait until an export success message is displayed on the top of the **Container Images** page. Find the exported file in the default download path on your local PC.

Do not close the browser page during the export, or the export will be interrupted.

----End

Exporting Repository Image Scan Results from the Image View

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 On the **Image View** tab page, select **Repository Images**, click **Export**, and select a risk type.

Figure 5-68 Exporting scan results

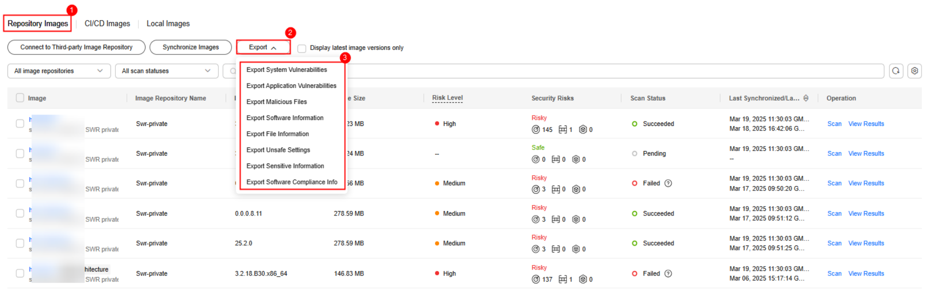

1
Repository Images
CI/CD Images
Local Images
Connect to Third-party Image Repository
Synchronize Images
2
Export
□ Display latest image versions only
3
Export System Vulnerabilities
Export Application Vulnerabilities
Export Malicious Files
Export Software Information
Export File Information
Export Unsafe Settings
Export Sensitive Information
Export Software Compliance Info
All image repositories
All scan statuses

Image	Image Repository Name	I	e Size	Risk Level	Security Risks	Scan Status	Last Synchronized/La...	Operation
[redacted] SWR private	Swr-private		23 MB	● High	Risky 145 1 0	Succeeded	Mar 19, 2025 11:30:03 GM... Mar 18, 2025 16:42:06 G...	Scan View Results
[redacted] SWR private	Swr-private		24 MB	--	Safe 0 0 0	Pending	Mar 19, 2025 11:30:03 GM... --	Scan View Results
[redacted] SWR private	Swr-private		56 MB	● Medium	Risky 3 0 0	Failed	Mar 19, 2025 11:30:03 GM... Mar 17, 2025 09:50:20 G...	Scan View Results
[redacted] SWR private	Swr-private	0.0.0.8.11	278.59 MB	● Medium	Risky 3 0 0	Succeeded	Mar 19, 2025 11:30:03 GM... Mar 17, 2025 09:51:12 G...	Scan View Results
[redacted] SWR private	Swr-private	25.2.0	278.59 MB	● Medium	Risky 3 0 0	Succeeded	Mar 19, 2025 11:30:03 GM... Mar 17, 2025 09:51:25 G...	Scan View Results
[redacted] hitecture SWR private	Swr-private	3.2.18.B30.x86_64	146.83 MB	● High	Risky 137 1 0	Failed	Mar 19, 2025 11:30:03 GM... Mar 06, 2025 15:17:14 G...	Scan View Results

Step 5 In the displayed dialog box, click **OK**.

Step 6 Wait until an export success message is displayed on the top of the **Container Images** page. Find the exported file in the default download path on your local PC.

Do not close the browser page during the export, or the export will be interrupted.

----End

5.3.4.6 Managing the Repository Image Vulnerability Whitelist

Scenarios

When adding a vulnerability to the whitelist, you need to specify the applicable scope of the whitelist item. If this item only applies to an image, the vulnerability will not be displayed in the scan results of this image, but will still be displayed under other images.

You can whitelist the image vulnerabilities that do not affect services.

You can add, modify, and delete repository image vulnerabilities in the whitelist.

Adding a Repository Image Vulnerability to the Whitelist

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In the upper right corner of the page, click **Configure Whitelist**.

You can also locate a vulnerability in **Risk View** or **Image View**, and click **Add to Whitelist** in its **Operation** column.

Step 5 On the **Repository Images** tab page, click **Add Rule**.

Step 6 On the **Add Rule** page, configure whitelist rule parameters. For details, see Table 5-33.

Table 5-33 Vulnerability whitelist rule parameters

Parameter	Description	Example Value
Type	Select a vulnerability type from the drop-down list. ● **Linux Vulnerabilities** ● **Application Vulnerabilities**	Linux Vulnerabilities
Vulnerability	Select a vulnerability from the drop-down list.	-
Image Scope	Select the applicable image scope of the whitelist item. ● **All**: all the images affected by the vulnerability ● **Specify types of image repositories**: specified image repositories affected by the vulnerability ● **Specific**: specific images affected by the vulnerability You can filter images by repository type or other criteria, and then select images.	Specific, Drupal
Remarks	Enter remarks to help you identify or trace whitelist operations.	test

Step 7 Click **OK**.

Step 8 Return to the repository image whitelist. Verify that the whitelisted vulnerability is displayed.

----End

Modifying a Repository Image Vulnerability in the Whitelist

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In the upper right corner of the page, click **Configure Whitelist**.

Step 5 Locate a whitelist item on the **Repository Images** tab.

Step 6 In the **Operation** column of the item, click **Edit**.

Step 7 On **Edit Whitelist Rule** page, modify the image scope and remarks.

Table 5-34 Parameters for modifying a whitelist rule

Parameter	Description	Example Value
Image Scope	Select the applicable image scope of the whitelist item. ● **All**: all images affected by the vulnerability ● **Specify types of image repositories**: specified image repositories affected by the vulnerability ● **Specific**: specific images affected by the vulnerability You can filter images by repository type or other criteria, and then select images.	Specific, drupal
Remarks	Enter remarks to help you identify or trace whitelisting operations.	test

Step 8 Click **OK**.

----End

Deleting a Repository Image Vulnerability from the Whitelist

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In the upper right corner of the page, click **Configure Whitelist**.

Step 5 Locate a whitelist item on the **Repository Images** tab.

Step 6 In the **Operation** column of the item, click **Delete**.

Step 7 In the displayed dialog box, confirm the whitelist information and click **OK**.

Step 8 Return to the image whitelist. Verify that the deleted whitelist item does not exist.

----End

5.3.5 Local Image Security Scan

5.3.5.1 Local Image Security Scan Overview

What Is a Local Image Security Scan?

Local images are stored or running on your container hosts. If they come from user-built repositories without security assurance, or be uploaded by developers without strict security review, they may have vulnerabilities or other risks that harm the production environment.

Local image security scan scans local images to detect security risks such as system vulnerabilities and application vulnerabilities and provides rectification suggestions, helping users reduce risks caused by non-compliant or invalid images.

Local Image Security Scan Principles

HSS embeds scan tools in images to access and parse their file systems, and to perform comprehensive security checks on files and directories. After the check is complete, all check results are summarized and reported to the management console.

Local Image Security Scan Items

The image security scan items are listed in **Table 5-35**.

Table 5-35 Local image security scan items

Scan Item	Description
Vulnerabilities	System and application vulnerabilities in images. ● System vulnerability scan supports the following OSs: – EulerOS 2.2, 2.3, 2.5, 2.8, 2.9, 2.10, 2.11, 2.12 (64-bit) – CentOS 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 (64-bit) – Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04 (64-bit) – Debian 9, 10, and 11 (64-bit) – Kylin V10, V10 SP1, and V10 SP2 (64-bit) – HCE 1.1 and 2.0 (64-bit) – SUSE 12 SP5, 15 SP1, and 15 SP2 (64-bit) – UnionTech OS V20 server E, V20 server D, 1050u2e, 1050e, 1060e (64-bit) – Rocky Linux 8.4, 8.5, 8.6, 8.10, 9.0, 9.1, 9.2, 9.4, and 9.5 (64-bit) – OpenEuler 20.03, 22.03, and 24.03 (64-bit) – CTyunOS 3-23.01 (64-bit) – AlmaLinux 8.4 (64-bit) ● Application vulnerability scan supports the following applications: Apache, Nginx, Tomcat, Kibana, mongo-express, yapi-cli, easy-mock, nodebb, kafka, rocketmq, Webasyst, KYPHP, CodeIgniter, InitPHP, SpeedPHP, ThinkPHP, OneThink, MySQL, Redis, Oracle, MongoDB, Memcache, PostgreSQL, DB2, Sybase, sshd and vsftpd.
Software Information	Software information in an image.

Scenarios

You can scan images in the production environment when your company or organizations deploy containerized applications.

Constraints

- Edition requirement: Only the HSS container edition supports local image security scan. You can scan images for an unlimited number of times. For details about how to purchase and upgrade an HSS edition, see **Purchasing an HSS Quota** and **Upgrading Protection Quotas**.
- Supported runtime: Only local Linux images in Docker and Containerd can be scanned.
- Storage drive requirements:
  - Docker: Only the image storage nodes using overlay and overlay2 can be scanned.

  - Containerd: Only the image storage nodes using OverlayFS can be scanned.
- Image storage path constraints:
  - Containerd: All local file system paths can be scanned.
  - Docker: By default, only the **/var/lib** directory is scanned. If the Docker root directory is not under this path, HSS cannot scan images. You are advised to perform image scans on Containerd servers.
- Name constraints: The images or versions whose names contain **--** cannot be scanned.
- To scan the **cce-pause/pause** image, HSS needs to start the **sh/bash** process. If the **cce-pause/pause** container does not have this process, the image scan task will fail. The **cce-pause/pause** container is a sandbox container. It has only one static compilation process and no vulnerabilities. Therefore, an image scan task failure does not affect services.

Local Image Security Scan Process

Figure 5-69 Usage process

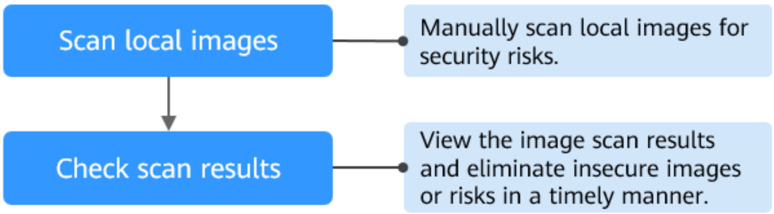

Scan local images
Manually scan local images for security risks.
Check scan results
View the image scan results and eliminate insecure images or risks in a timely manner.

Table 5-36 Process description

Operation	Description
Scanning Local Images	After the HSS agent is installed on a cluster node, the agent immediately starts synchronizing local image information to the HSS console. The information is updated every 24 hours. After the local image information is displayed, you can manually scan the images.
Viewing and Handling Local Image Scan Results	View the local image scan results, and fix insecure images and risks, so that they will not harm the production environment.

5.3.5.2 Scanning Local Images

Scenarios

After the HSS agent is installed on a cluster node, the agent immediately starts synchronizing local image information to the HSS console. The information is updated every 24 hours.

After the local image information is displayed, you can manually scan the images.

Manually Scanning Local Images

Step 1 Log in to the management console.

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

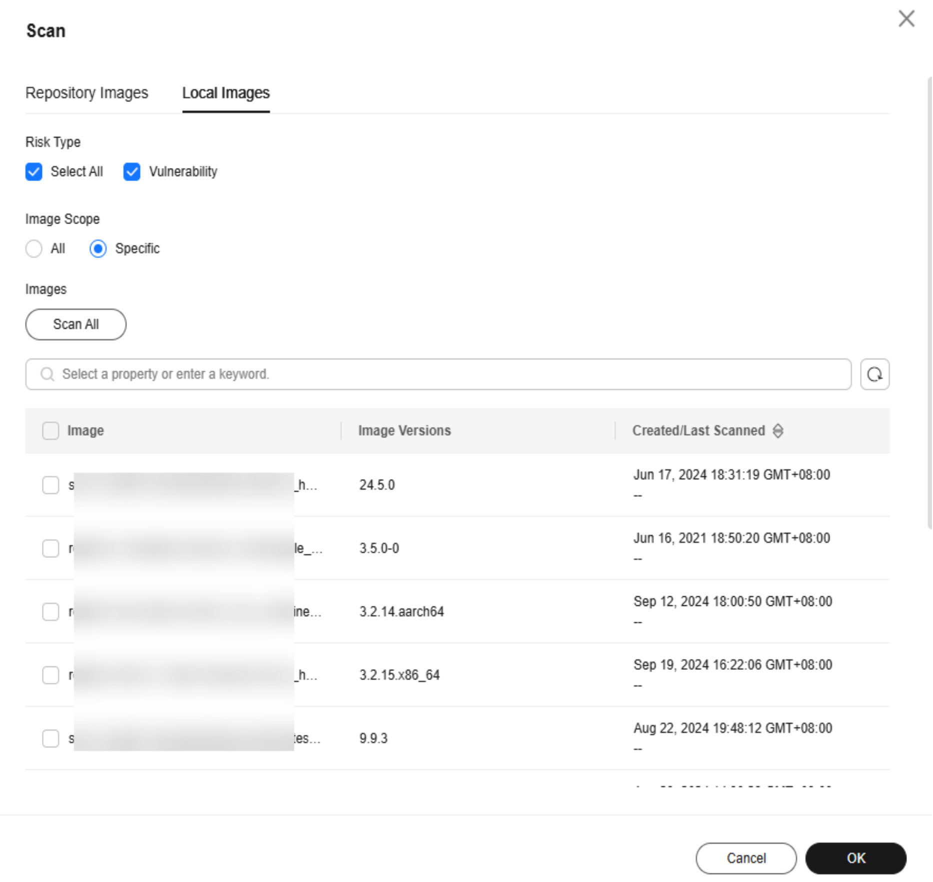
Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In the upper right corner of the page, click **Scan**.

To scan a single image, click the **Image View** tab, click **Scan** in the **Operation** column of the image.

Step 5 Click the **Local Images** tab and configure parameters. For details, see **Table 5-37**.

Figure 5-70 Manually scanning local images



Scan

Repository Images | Local Images

Risk Type

☑ Select All ☑ Vulnerability

Image Scope

○ All ● Specific

Images

Scan All

Select a property or enter a keyword.

□ Image	Image Versions	Created/Last Scanned
□ [redacted]	24.5.0	Jun 17, 2024 18:31:19 GMT+08:00 --
□ [redacted]	3.5.0-0	Jun 16, 2021 18:50:20 GMT+08:00 --
□ [redacted]	3.2.14.aarch64	Sep 12, 2024 18:00:50 GMT+08:00 --
□ [redacted]	3.2.15.x86_64	Sep 19, 2024 16:22:06 GMT+08:00 --
□ [redacted]	9.9.3	Aug 22, 2024 19:48:12 GMT+08:00 --

Table 5-37 Local image scan parameters

Parameter	Description	Example Value
Risk Type	Select **Vulnerability**, if needed. HSS scans for software information by default. You do not need to select it.	Selected
Image Scope	Select **All** or **Specific**. A full scan takes a long time and cannot be stopped once started. Exercise caution when performing this operation.	All

Step 6 Click **OK**.

Step 7 In the upper right corner of the page, click **Manage Task** Click the **Image Scan** tab to view the scan status.

The duration of a security scan depends on the scanned image size. Generally, an image can be scanned within 3 minutes.

Step 8 After the image scan task is complete, return to **Image View**. You can view the scan status of each image. For details, see **Table 5-38**.

Table 5-38 Risk status

Status	Description
Pending	The image is not scanned.
Scanning	The image is being scanned.
Succeeded	The image has been scanned. You can view the scan results.
Failed	An error or problem occurred during image scan. As a result, the scan failed.
To be scanned	A scan task has been created, and the image is waiting to be scanned.
Scan terminated	The scan task has been canceled, and the image scan has been stopped.

----End

Stopping a Scan Task

You can stop a running scan task.

Constraints

- The following permissions are required for stopping a scan:
  - HSS permission: batch image scan (hss:images:set) or container asset management (hss:containers:set)

- Namespace permission (Kubernetes RBAC): the permission for deleting **job** or **cronjob** resources in HSS namespaces

Procedure

Step 1 In the upper right corner of the **Container Images** page, click **Manage Task**.

Step 2 Click the **Image Scan** tab.

Step 3 In the **Operation** column of a task, click **Cancel Scan**.

Step 4 If **Cancelled** is displayed in the **Scan Status** column of the task, the scan has been canceled.

----End

5.3.5.3 Viewing and Handling Local Image Scan Results

Scenarios

HSS can present image security statistics in the risk view and image view, helping you comprehensively learn, locate, and fix image risks.

- Risk view: View all the scan results of a risk. Local image risks include system vulnerabilities and application vulnerabilities.
- Image view: View the scan results of a single image. Local image scan results include system vulnerabilities, application vulnerabilities, and software information.

You can view and handle local image scan results in **Risk View** or **Image View**.

Viewing and Handling Local Scan Results in the Risk View

Step 1 Log in to the management console.

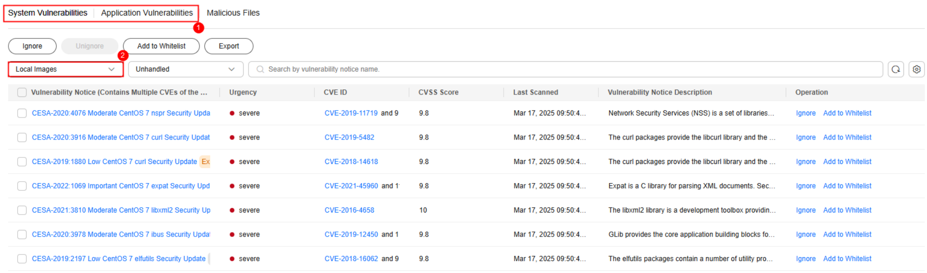
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In **Risk View**, click **System Vulnerabilities**, **Application Vulnerabilities**, or **Software Information**. Filter **Local images**, and view and handle the scan results. For details, see **Table 5-39**.

Image names are not displayed in software information. You can export scan results to obtain these image names and image tags.

Figure 5-71 Local image risk view



Vulnerability Notice (Contains Multiple CVEs of the ...	Urgency	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
CESA-2020:4076 Moderate CentOS 7 nspr Security Upda	● severe	CVE-2019-11719 and 9	9.8	Mar 17, 2025 09:50:4...	Network Security Services (NSS) is a set of libraries...	Ignore Add to Whitelist
CESA-2020:3916 Moderate CentOS 7 curl Security Updat	● severe	CVE-2019-5482	9.8	Mar 17, 2025 09:50:4...	The curl packages provide the libcurl library and the ...	Ignore Add to Whitelist
CESA-2019:1880 Low CentOS 7 curl Security Update Ex	● severe	CVE-2018-14618	9.8	Mar 17, 2025 09:50:4...	The curl packages provide the libcurl library and the ...	Ignore Add to Whitelist
CESA-2022:1069 Important CentOS 7 expat Security Upd	● severe	CVE-2021-45960 and 1	9.8	Mar 17, 2025 09:50:4...	Expat is a C library for parsing XML documents. Sec...	Ignore Add to Whitelist
CESA-2021:3810 Moderate CentOS 7 libxml2 Security Up	● severe	CVE-2016-4658	10	Mar 17, 2025 09:50:4...	The libxml2 library is a development toolbox providin...	Ignore Add to Whitelist
CESA-2020:3978 Moderate CentOS 7 ibus Security Updat	● severe	CVE-2019-12450 and 1	9.8	Mar 17, 2025 09:50:4...	GLib provides the core application building blocks fo...	Ignore Add to Whitelist
CESA-2019:2197 Low CentOS 7 elfutils Security Update	● severe	CVE-2018-16062 and 9	9.8	Mar 17, 2025 09:50:4...	The elfutils packages contain a number of utility pro...	Ignore Add to Whitelist

Table 5-39 Local image scan result parameters

Risk Type	Description
Vulnerability risks (system and application vulnerabilities)	Results of OS and application vulnerability scans. You can perform the following operations: ● View vulnerability details Click a vulnerability notice name. On the vulnerability details page, view the vulnerability notice, CVE (for system vulnerabilities only), suggestions, affected images, and handling history. ● Handle vulnerabilities – Ignore If a vulnerability does not need to be handled for now, you can ignore it. It will still be displayed in future scan results. – Add to whitelist If a vulnerability does not affect your services, you can add it to the whitelist. – Fix Fix the vulnerability by referring to the suggestions in the vulnerability details.

----End

Viewing and Handling Local Scan Results in the Image View

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 Click the **Image View** tab.

Figure 5-72 Image view

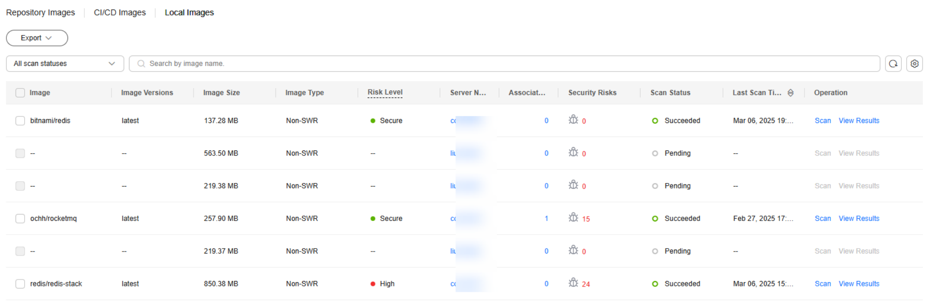


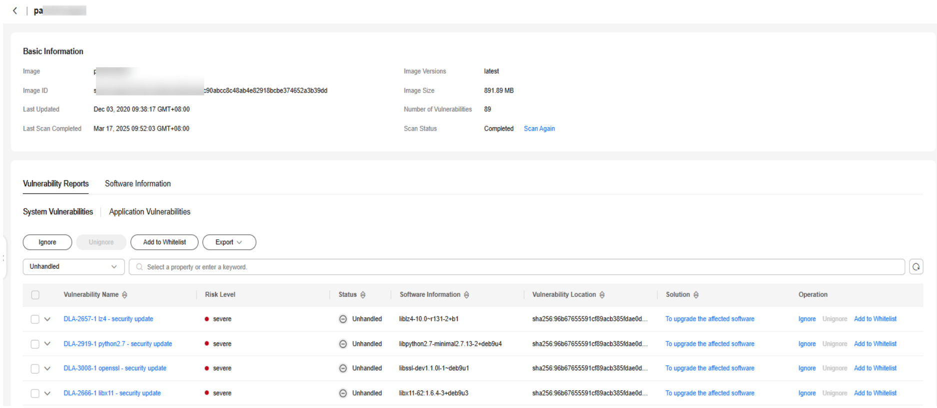
Image	Image Versions	Image Size	Image Type	Risk Level	Server N...	Associat...	Security Risks	Scan Status	Last Scan Ti...	Operation
bitnami/redis	latest	137.28 MB	Non-SWR	● Secure	[redacted]	0	0	○ Succeeded	Mar 06, 2025 19:...	Scan View Results
--	--	563.50 MB	Non-SWR	--	[redacted]	0	0	○ Pending	--	Scan View Results
--	--	219.38 MB	Non-SWR	--	[redacted]	0	0	○ Pending	--	Scan View Results
ochh/rocketmq	latest	257.90 MB	Non-SWR	● Secure	[redacted]	1	15	○ Succeeded	Feb 27, 2025 17:...	Scan View Results
--	--	219.37 MB	Non-SWR	--	[redacted]	0	0	○ Pending	--	Scan View Results
redis/redis-stack	latest	850.38 MB	Non-SWR	● High	[redacted]	0	24	○ Succeeded	Mar 06, 2025 15:...	Scan View Results

Step 5 Click the **Local Images** tab.

Step 6 In the **Operation** column of an image, click **View Results** to go to the image details page.

Step 7 View and handle risk scan results. For details, see **Table 5-40**.

Figure 5-73 Local image scan details



pa[redacted]

Basic Information

Image	p[redacted]	Image Versions	latest
Image ID	s[redacted]c90abcc8c48ab4e82918bcbe374652a3b39dd	Image Size	891.89 MB
Last Updated	Dec 03, 2020 09:38:17 GMT+08:00	Number of Vulnerabilities	89
Last Scan Completed	Mar 17, 2025 09:52:03 GMT+08:00	Scan Status	Completed Scan Again

Vulnerability Name	Risk Level	Status	Software Information	Vulnerability Location	Solution	Operation
DLA-2657-1 lz4 - security update	● severe	Unhandled	liblz4-10.0~r131-2+b1	sha256:96b67655591cf89acb385fdae0d...	To upgrade the affected software	Ignore Unignore Add to Whitelist
DLA-2919-1 python2.7 - security update	● severe	Unhandled	libpython2.7-minimal2.7.13-2+deb9u4	sha256:96b67655591cf89acb385fdae0d...	To upgrade the affected software	Ignore Unignore Add to Whitelist
DLA-3008-1 openssl - security update	● severe	Unhandled	libssl-dev1.1.0l-1~deb9u1	sha256:96b67655591cf89acb385fdae0d...	To upgrade the affected software	Ignore Unignore Add to Whitelist
DLA-2666-1 libx11 - security update	● severe	Unhandled	libx11-62:1.6.4-3+deb9u3	sha256:96b67655591cf89acb385fdae0d...	To upgrade the affected software	Ignore Unignore Add to Whitelist

Table 5-40 Local image scan result parameters

Risk Type	Description
Vulnerability Reports	Results of OS and application vulnerability scans. You can perform the following operations: ● View vulnerability details Click a vulnerability name to go to its details page. View the vulnerability description, urgency, and affected images. ● Handle vulnerabilities – Ignore If a vulnerability does not need to be handled for now, you can ignore it. It will still be displayed in future scan results. – Add to whitelist If a vulnerability does not affect your services, you can add it to the whitelist. – Fix To fix a system vulnerability, upgrade the software affected by it. Click **To upgrade the affected software** to go to the security notice details page. View the affected components, CVE, and more information. To fix an application vulnerability, hover the cursor over the solution description of a vulnerability to view the solution. To install a patch, access the patch installation guide link provided in the solution, and install the patch accordingly.
Software Information	Statistical results of image software, including the software names, types, versions, and number of software vulnerabilities. Click ∨ next to a software name to view its vulnerability name, urgency, and solution.

----End

5.3.5.4 Exporting Local Image Scan Results

Scenarios

Export image scan results to a local PC.

Exporting Local Image Scan Results from the Risk View

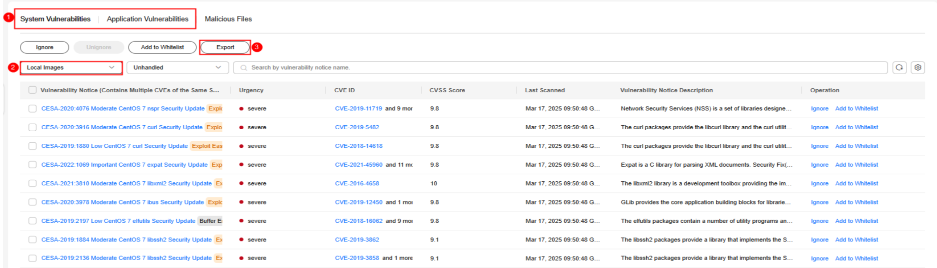
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In **Risk View**, click **System Vulnerabilities**, **Application Vulnerabilities**, or **Software Information**. Filter **Local images**, and click **Export**.

Figure 5-74 Exporting scan results



□ Vulnerability Notice (Contains Multiple CVEs of the Same S...	Urgency	CVE ID	CVSS Score	Last Scanned	Vulnerability Notice Description	Operation
□ CESA-2020:4076 Moderate CentOS 7 nspr Security Update Explo	● severe	CVE-2019-11719 and 9 mor	9.8	Mar 17, 2025 09:50:48 G...	Network Security Services (NSS) is a set of libraries designe...	Ignore Add to Whitelist
□ CESA-2020:3916 Moderate CentOS 7 curl Security Update Explo	● severe	CVE-2019-5482	9.8	Mar 17, 2025 09:50:48 G...	The curl packages provide the libcurl library and the curl utilit...	Ignore Add to Whitelist
□ CESA-2019:1880 Low CentOS 7 curl Security Update Exploit Eas	● severe	CVE-2018-14618	9.8	Mar 17, 2025 09:50:48 G...	The curl packages provide the libcurl library and the curl utilit...	Ignore Add to Whitelist
□ CESA-2022:1069 Important CentOS 7 expat Security Update Exp	● severe	CVE-2021-45960 and 11 mc	9.8	Mar 17, 2025 09:50:48 G...	Expat is a C library for parsing XML documents. Security Fix(...	Ignore Add to Whitelist
□ CESA-2021:3810 Moderate CentOS 7 libxml2 Security Update Ex	● severe	CVE-2016-4658	10	Mar 17, 2025 09:50:48 G...	The libxml2 library is a development toolbox providing the im...	Ignore Add to Whitelist
□ CESA-2020:3978 Moderate CentOS 7 ibus Security Update Explo	● severe	CVE-2019-12450 and 1 mor	9.8	Mar 17, 2025 09:50:48 G...	GLib provides the core application building blocks for librarie...	Ignore Add to Whitelist
□ CESA-2019:2197 Low CentOS 7 elfutils Security Update Buffer E	● severe	CVE-2018-16062 and 9 mor	9.8	Mar 17, 2025 09:50:48 G...	The elfutils packages contain a number of utility programs an...	Ignore Add to Whitelist
□ CESA-2019:1884 Moderate CentOS 7 libssh2 Security Update Ex	● severe	CVE-2019-3862	9.1	Mar 17, 2025 09:50:48 G...	The libssh2 packages provide a library that implements the S...	Ignore Add to Whitelist
□ CESA-2019:2136 Moderate CentOS 7 libssh2 Security Update Ex	● severe	CVE-2019-3858 and 1 more	9.1	Mar 17, 2025 09:50:48 G...	The libssh2 packages provide a library that implements the S...	Ignore Add to Whitelist

Step 5 In the displayed dialog box, click **OK**.

Step 6 Wait until an export success message is displayed on the top of the **Container Images** page. Find the exported file in the default download path on your local PC.

Do not close the browser page during the export, or the export will be interrupted.

----End

Exporting Local Image Scan Results from the Image View

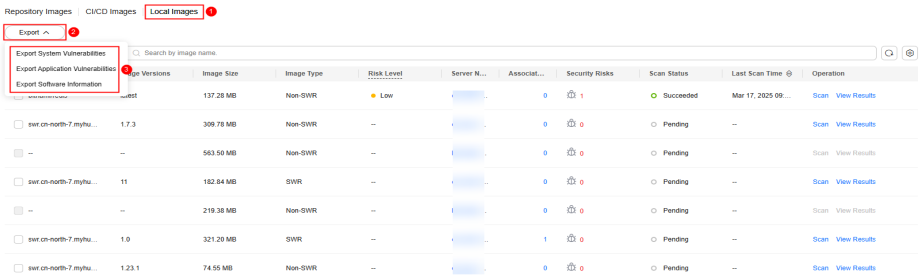
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 On the **Image View** tab page, select **Local Images**, click **Export**, and select a risk type.

Figure 5-75 Exporting scan results


Repository Images
CI/CD Images
Local Images
1
Export
2
Export System Vulnerabilities
Export Application Vulnerabilities
3
Export Software Information
Search by image name.

	ge Versions	Image Size	Image Type	Risk Level	Server N...	Associat...	Security Risks	Scan Status	Last Scan Time	Operation
	atest	137.28 MB	Non-SWR	● Low	[redacted]	0	1	○ Succeeded	Mar 17, 2025 09:...	Scan View Results
□ swr.cn-north-7.myhu...	1.7.3	309.78 MB	Non-SWR	--	[redacted]	0	0	○ Pending	--	Scan View Results
□ --	--	563.50 MB	Non-SWR	--	[redacted]	0	0	○ Pending	--	Scan View Results
□ swr.cn-north-7.myhu...	11	182.84 MB	SWR	--	[redacted]	0	0	○ Pending	--	Scan View Results
□ --	--	219.38 MB	Non-SWR	--	[redacted]	0	0	○ Pending	--	Scan View Results
□ swr.cn-north-7.myhu...	1.0	321.20 MB	SWR	--	[redacted]	1	0	○ Pending	--	Scan View Results
□ swr.cn-north-7.myhu...	1.23.1	74.55 MB	Non-SWR	--	[redacted]	0	0	○ Pending	--	Scan View Results

Step 5 In the displayed dialog box, click **OK**.

Step 6 Wait until an export success message is displayed on the top of the **Container Images** page. Find the exported file in the default download path on your local PC.

Do not close the browser page during the export, or the export will be interrupted.

----End

5.3.5.5 Managing the Local Image Vulnerability Whitelist

Scenarios

When adding a vulnerability to the whitelist, you need to specify the applicable scope of the whitelist item. If this item only applies to an image, the vulnerability will not be displayed in the scan results of this image, but will still be displayed under other images.

You can whitelist the image vulnerabilities that do not affect services.

You can add, modify, and delete local image vulnerabilities in the whitelist.

Adding a Local Image Vulnerability to the Whitelist

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In the upper right corner of the page, click **Configure Whitelist**.

You can also locate a vulnerability in **Risk View** or **Image View**, and click **Add to Whitelist** in its **Operation** column.

Step 5 On the **Local Images** tab page, click **Add Rule**.

Step 6 On the **Add Rule** page, configure whitelist rule parameters. For details, see **Table 5-41**.

Table 5-41 Vulnerability whitelist rule parameters

Parameter	Description	Example Value
Type	Select a vulnerability type from the drop-down list. ● **Linux Vulnerabilities** ● **Application Vulnerabilities**	**Linux Vulnerabilities**
Vulnerability	Select a vulnerability from the drop-down list.	-
Image Scope	Select the applicable image scope of the whitelist item. ● **All**: all images affected by the vulnerability ● **Specific**: specific images affected by the vulnerability You can filter images by their source or other conditions, and then select images.	Specific, Drupal
Remarks	Enter remarks to help you identify or trace whitelisting operations.	test

Step 7 Click **OK**.

Step 8 Return to the local image whitelist. Verify that the whitelisted vulnerability is displayed.

----End

Modifying a Local Image Vulnerability in the Whitelist

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

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In the upper right corner of the page, click **Configure Whitelist**.

Step 5 Locate a whitelist item on the **Local Images** tab.

Step 6 In the **Operation** column of the whitelist, click **Edit**.

Step 7 On **Edit Whitelist Rule** page, modify the image scope and remarks.

Table 5-42 Parameters for modifying a whitelist rule

Parameter	Description	Example Value
Image Scope	Select the applicable image scope of the whitelist item. ● **All**: all images affected by the vulnerability ● **Specific**: specific images affected by the vulnerability You can filter images by their source or other conditions, and then select images.	Specific, Drupal
Remarks	Enter remarks to help you identify or trace whitelisting operations.	test

Step 8 Click **OK**.

----End

Deleting a Local Image Vulnerability from the Whitelist

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Container Images**.

Step 4 In the upper right corner of the page, click **Configure Whitelist**.

Step 5 Locate a whitelist item on the **Local Images** tab.

Step 6 In the **Operation** column of the item, click **Delete**.

Step 7 In the displayed dialog box, confirm the whitelist information and click **OK**.

Step 8 Return to the image whitelist. Verify that the deleted whitelist item does not exist.

----End

5.4 Cluster Environment Security

5.4.1 Cluster Environment Security Overview

What Is Cluster Environment Security?

A cluster is a combination of cloud resources, such as cloud servers and load balancers, for container running. A cluster can be seen as one or more elastic cloud servers (nodes) in a same subnet. It provides compute resources for running containers.

Cluster environment security scans the resources on the Kubernetes cluster management plane and data plane; identifies infrastructure as code (IaC) risks, vulnerabilities, unsafe settings, configuration compliance, sensitive information, and permissions management issues; and provides solutions, helping you build a comprehensive cluster security system.

Regarding cluster security, the following items are checked:

- System vulnerabilities: The vulnerabilities at the OS layer of the core components in the control plane, data plane, and image repositories of Kubernetes clusters.
- Application software vulnerabilities: The application vulnerabilities in the core components of the Kubernetes cluster control plane, data plane, and image repositories.
- Emergency vulnerabilities: The high-risk security vulnerabilities, such as 0-day vulnerabilities, in containers, container runtime components, and dependency packages.
- Unsafe configuration: Kubernetes cluster settings, workloads, network policies, and role-based access control (RBAC) permissions are comprehensively checked to ensure that cluster deployment complies with best security practices.
- Security and compliance: The security and compliance of Kubernetes cluster settings, workloads, network policies, and RBAC permissions are checked to ensure that cluster deployment complies with industry standards and regulations.
- IaC risks: The risks in infrastructure as code (IaC).

System and Application Vulnerability Scan Principles

HSS obtains the container images used by the core components of the Kubernetes cluster control plane, data plane, and image repositories. It scans these images for application and system vulnerabilities. For more information, see **Table 5-43**.

Table 5-43 Cluster components scanned by HSS

Namespace	Component
kube-system	kube-apiserver, kube-controller-manager, kube-scheduler, etcd, kube-proxy, coredns, metrics-server, calico/node, weaveworks/weave-kube
goharbor	harbor-core, harbor-portal, harbor-registry, harbor-jobservice, trivy-adapter, redis, postgresql
docker.bintray.io	artifactory-pro, fluentd, bitnami/nginx
releases.jfrog.io	artifactory-pro, xray-server, pipelines, distribution

If the preceding components in a cluster are not running in containers or the cluster network is unreachable, the cluster cannot be scanned for system and application vulnerabilities.

- The following OSs can be scanned for system vulnerabilities:
  - EulerOS 2.2, 2.3, 2.5, 2.8, 2.9, 2.10, 2.11, 2.12 (64-bit)
  - CentOS 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 (64-bit)
  - Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04 (64-bit)
  - Debian 9, 10, and 11 (64-bit)
  - Kylin V10, V10 SP1, and V10 SP2 (64-bit)
  - HCE 1.1 and 2.0 (64-bit)
  - SUSE 12 SP5, 15 SP1, and 15 SP2 (64-bit)
  - UnionTech OS V20 server E, V20 server D, 1050u2e, 1050e, 1060e (64-bit)
  - Rocky Linux 8.4, 8.5, 8.6, 8.10, 9.0, 9.1, 9.2, 9.4, and 9.5 (64-bit)
  - OpenEuler 20.03, 22.03, and 24.03 (64-bit)
  - CTyunOS 3-23.01 (64-bit)
  - AlmaLinux 8.4 (64-bit)
- The following applications and middleware can be scanned for application vulnerabilities: log4j, slf4j, tomcat, apache, jetty, mysql, druid, commons, spring, shiro, struts, struts2, websocket, json, fastjson, xstream, maven, junit, activemq, libintl, ca-certificates-java, httpclient, httpcore, java, javac2, javaee, Apache2, adaptive_server_enterprise, DB2, http_server, Memcached, nginx, PostgreSQL, bootstrap, zookeeper, plexus-utils, and core.

Unsafe Configuration and Compliance Scan Principles

To identify unsafe configuration and non-compliance issues, HSS uses a pre-defined security framework and dynamic policy engine to perform in-depth checks on Kubernetes cluster configuration, workloads, network policies, and RBAC permissions. The two types of issues are checked in different dimensions and scenarios. For details, see **Table 5-44**.

Table 5-44 Comparison between unsafe configuration checks and compliance checks

Difference	Unsafe Configuration	Security and Compliance
Dimension	Based on Huawei Cloud's years of experience in cloud security, this service checks the configuration of Kubernetes components, workloads, network policies, and more resources, helping to ensure it complies with best security practices.	Based on industry standards and regulations, this service checks the configuration of Kubernetes components, workloads, network policies, and more resources, helping to ensure it meets security and compliance requirements.

Difference	Unsafe Configuration	Security and Compliance
Risk type	Control plane, access control, key management, network, workload, and node escape. For details, see **Table 5-45**.	Control plane, access control, network, and workload. For details, see **Table 5-45**.
Scenario	Security assurance during critical periods or events. A comprehensive evaluation can be performed on a cluster, helping to ensure each of its components uses the recommended security configuration, thereby reducing risks.	Compliance check. It helps to ensure the configuration of each component in a cluster complies with industry standards and existing laws and regulations, reducing compliance risks.

Table 5-45 describes the types of risks that can be detected in unsafe configuration checks and compliance checks.

Table 5-45 Risk types

Risk Type	Description
Control plane	Check the security of Kubernetes control plane components, including API Server, Controller Manager, Scheduler, and etcd. For example, check whether etcd data is encrypted.
Access control	Check the security rules related to Kubernetes authentication, authorization, and RBAC configuration. For example, check whether a user or account has excessive permissions.
Key management	Check how secrets are stored, used, and protected in Kubernetes. For example, check whether the access to secrets is restricted.
Network	Check the Kubernetes network policies and security rules related to inter-service communication. For example, check whether a proper network policy is defined to restrict the communication between pods.
Workload	Check the security configuration of workloads, such as pods, Deployments, StatefulSets, and DaemonSets. For example, check whether containers are run by non-root users.
Node escape	Check whether there are security risks that can be exploited by attackers to escape from containers to hosts. For example, check whether the Docker socket (/var/run/docker.sock) is mounted.

Emergency Vulnerability Scan Principles

Version comparison and PoC verification are performed to check for vulnerabilities in runc and other container runtime components, dependency packages, and the software running in containers.

IaC Risk Scan Principles

The Infrastructure as Code (IaC) files uploaded by users are checked against the built-in IaC risk rule library to detect risks.

Currently, the following file types can be scanned: Dockerfile (image configuration file) and Kubernetes YAML (cluster resource configuration file).

Application Scenarios of Cluster Environment Security

- **Improving cluster environment security**

  Scan the cluster environment to detect and fix security vulnerabilities, unsafe settings, and IaC risks as soon as possible, improving environment security and reducing intrusion risks.
- **Ensuring cluster environment compliance**

  Cluster environment security scans help you ensure that containerized applications and related settings comply with the strict regulations and standards in different industries.
- **Improving the quality of containerized applications and services**

  Regular cluster security scans and problem rectification help the development team better understand related specifications, improving the development quality and efficiency of containerized applications and services.

Constraints

- **Kubernetes cluster version**: Cluster security scans are supported for version 1.19 and later.
- **Prerequisites for IaC risk scan**: You have purchased the container edition. For details, see **Purchasing an HSS Quota**.
- **Prerequisites for the scans for system vulnerabilities, application vulnerabilities, unsafe configuration, and security & compliance**:

  a. The cluster has been connected to HSS and the connection is normal. For details, see **Overview of Agent Installation in a Cluster**.

  b. At least one node in the cluster is protected by the container edition. For details, see **Enabling Protection**.
- **Prerequisites for emergency vulnerability scans**: The nodes to be scanned are protected by the container edition. For details, see **Enabling Protection**.

Cluster Environment Scan Process

Figure 5-76 Usage process

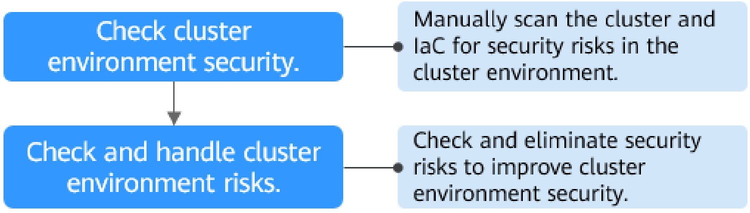

Check cluster environment security.
Manually scan the cluster and IaC for security risks in the cluster environment.
Check and handle cluster environment risks.
Check and eliminate security risks to improve cluster environment security.

Table 5-46 Usage process

Operation	Description
Checking Cluster Environment Security	Manually scan clusters and IaC for risks.
Viewing and Handling Security Risks in a Cluster	Check the security scan results and mitigate risks in the cluster environment in a timely manner.

5.4.2 Checking Cluster Environment Security

Scenarios

If a node in a cluster is protected by the container edition, you can check the cluster environment for IaC risks, vulnerabilities, configuration risks, sensitive information, and permissions management issues.

Checking Cluster Environment Security

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

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Cluster Environment**.

Step 4 In the upper right corner of the page, click **Scan**.

Step 5 Select risk types and configure the scan task as needed.

- **Scans for system vulnerabilities, application vulnerabilities, configuration risks, and compliance issues**:

  a. Click the **Cluster Scan** tab.

  b. Configure scan task parameters.

     For more information, see **Table 5-47**.

Table 5-47 Parameters of the scans for system vulnerabilities, application vulnerabilities, configuration risks, and compliance issues

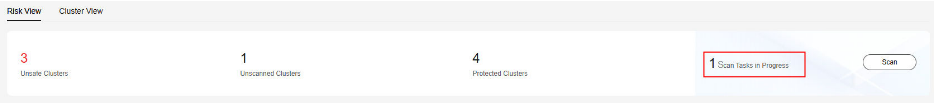
Parameter	Description	Example Value
Object Type	Select **Cluster**.	Cluster
Risk Type	Select **Cluster vulnerability**, **Configuration risk**, and **Security and Compliance** as needed. Cluster vulnerabilities include system and application vulnerabilities. For details about the risk items, see **Cluster Environment Security Overview**.	Select All
Cluster Scope	Select the cluster scope to be scanned. ▪ **All Clusters** All the clusters where at least one node is protected by the container edition. ▪ **Specific** Select clusters as needed.	All Clusters

c. Select **I understand that starting a cluster scan will authorize HSS to create the following resources on the Kubernetes cluster: Job, ConfigMap, ServiceAccount, ClusterRole, and ClusterRoleBinding**. For details about the usage of the created resources, see **Resource Creation Description**.

d. Click **Scan**.

e. In the upper right corner of the **Cluster Environment** page, view the execution progress of the scan task. See **Figure 5-77**.

Figure 5-77 Scan task execution status



- **Scan for emergency vulnerabilities**

  a. Click the **Cluster Scan** tab.

  b. Configure scan task parameters.

  For more information, see **Table 5-48**.

Table 5-48 Emergency vulnerability scan parameters

Parameter	Description	Example Value
Object Type	Select **Nodes**.	Nodes
Risk Type	**Emergency Vulnerabilities** is selected by default. No manual operations required.	Emergency Vulnerabilities
Nodes Scanned	Select the node scope to be scanned. ▪ All nodes All the nodes protected by the container edition. ▪ Specific nodes Select nodes as needed.	All nodes

c. Click **Scan**.

d. In the upper right corner of the **Cluster Environment** page, click **Manage Task**. On the displayed page, click **Cluster Scan** to view the scan task progress.

   After the scan task is complete, click **View Details** in the **Operation** column of a scan task to view the scan result of each node.

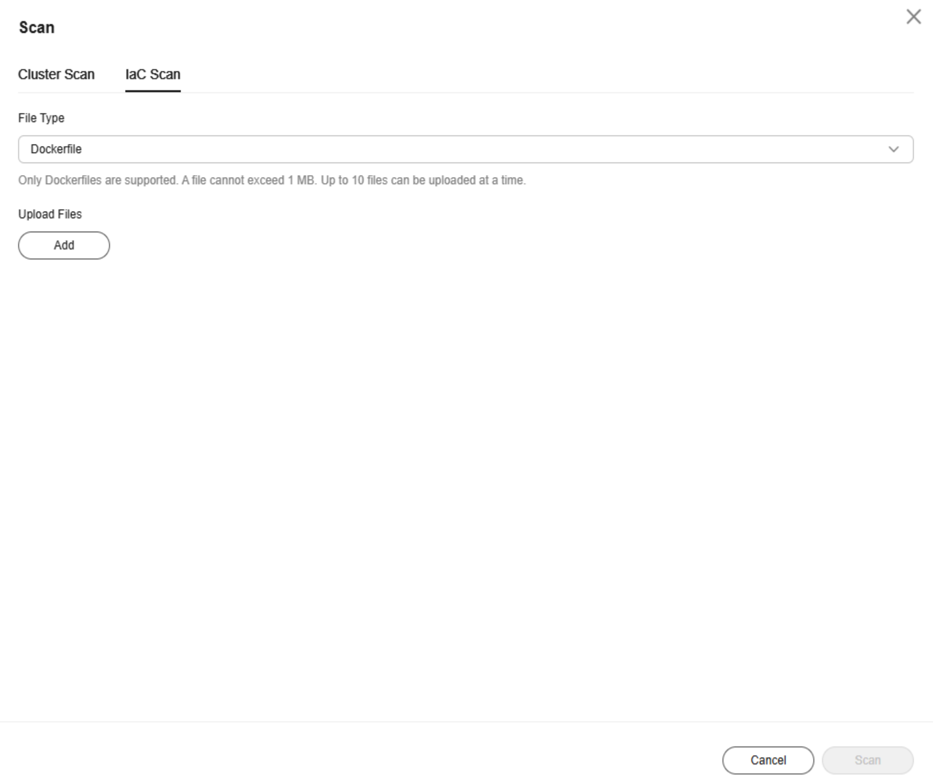
- **IaC risk scan**

  a. Click the **IaC Scan** tab.

  b. Configure scan task parameters.

     For more information, see **Table 5-49**.

Figure 5-78 IaC scan



Scan

Cluster Scan | IaC Scan

File Type

Dockerfile

Only Dockerfiles are supported. A file cannot exceed 1 MB. Up to 10 files can be uploaded at a time.

Upload Files

Table 5-49 IaC scan parameters

Parameter	Description
File Type	Select a file type from the drop-down list. The options are as follows: ▪ **Dockerfiles**: image configuration file ▪ **Kubernetes YAML**: cluster resource configuration file
Upload Files	Click **Add** and upload the files to be scanned. The requirements are as follows: ▪ A file cannot exceed 1 MB. Up to 10 files can be uploaded at a time. ▪ If a file is being scanned, wait until the scan is complete and then upload files.

c. Click **Scan**.

d. In the upper right corner of the **Cluster Environment** page, click **Manage Task**. On the displayed page, click **IaC Scan** to view the scan task progress.

After the scan task is complete, click **View Details** in the **Operation** column of a scan task to view the scan result of each file.

----End

Resource Creation Description

If you scan for system vulnerabilities, application vulnerabilities, configuration risks, or security and compliance issues, HSS will create resources in the cluster and use them for the scan, as described in **Table 5-50**. These resources will be automatically deleted after the scan task is complete.

- CCE clusters: When creating a scan task, you need to grant HSS the permission to create the resources described in **Table 5-50**.
- Other clusters: When you connect these clusters to HSS, you already grant HSS the permission to create the resources described in **Table 5-50**. When creating a scan task, you need to confirm that you acknowledge and accept the resources created by HSS. For details about the cluster resource permissions of HSS, see **Viewing the Cluster Node List and Permission List**.

Table 5-50 Resources and their usage in the scans for system vulnerabilities, application vulnerabilities, configuration risks, and compliance issues

Resource Type	Resource Name	Name space	Description
Job	cluster-scan-job-{id}	hss	Risk scan task. The ID in the name is the unique ID of a scan task.
ConfigMap	cluster-scan-configmap-{id}	hss	Scan task configuration. The ID in the name is the unique ID of a scan task.
ServiceAccount	hss-read-only-sa	hss	Account bound to a job to grant the job the read-only permission to query Kubernetes resources.
ClusterRoleBinding	hss-view-cluster-role-binding	-	Used to bind the permission of the internal cluster role **view** to **hss-read-only-sa**.
ClusterRole	hss-read-only-cluster-role	-	Used to create a role with the read-only permission for the following resource types to perform RBAC permission checks: roles, rolebindings, clusterroles, clusterrolebindings, validatingwebhookconfigurations, mutatingwebhookconfigurations, networkpolicies, podtemplates, secrets, nodes, leases, and csistoragecapacities

Resource Type	Resource Name	Name space	Description
ClusterRoleBinding	hss-read-only-binding	-	Used to bind the permissions of the **hss-read-only-cluster-role** role to **hss-read-only-sa**.

Follow-up Operations

After a scan task is complete, check and mitigate environment security risks. For details, see **Viewing and Handling Security Risks in a Cluster**.

5.4.3 Viewing and Handling Security Risks in a Cluster

Scenarios

HSS can present risks in the risk view or image view. This helps you comprehensively learn the risk status of the cluster environment and implement one-stop management of the cluster security posture.

- Risk view: View all the scan results of a risk, for example, a system vulnerability, application vulnerability, emergency vulnerability, configuration risk, security and compliance issue, or an IaC risk.
- Cluster view: View the scan results of a cluster, including its system vulnerabilities, application vulnerabilities, emergency vulnerabilities, configuration risks, and security and compliance issues.

This section describes how to view and handle cluster security risks in the risk view and the cluster view.

Viewing and Handling Cluster Environment Risks in the Risk View

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

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

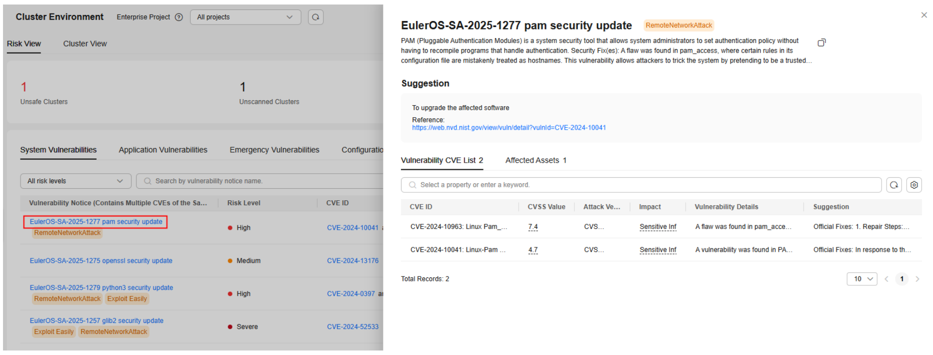
Step 3 In the navigation pane on the left, choose **Risk Management** > **Cluster Environment**.

Step 4 On the **Risk View** tab page, view and handle all types of security risks. They include:

- **System vulnerabilities**

  OS vulnerability scan results.

Figure 5-79 System vulnerabilities



Vulnerability Notice (Contains Multiple CVEs of the Sa...	Risk Level	CVE ID
EulerOS-SA-2025-1277 pam security update RemoteNetworkAttack	● High	CVE-2024-10041
EulerOS-SA-2025-1275 openssl security update	● Medium	CVE-2024-13176
EulerOS-SA-2025-1279 python3 security update RemoteNetworkAttack Exploit Easily	● High	CVE-2024-0397
EulerOS-SA-2025-1257 glib2 security update Exploit Easily RemoteNetworkAttack	● Severe	CVE-2024-52533

EulerOS-SA-2025-1277 pam security update RemoteNetworkAttack

PAM (Pluggable Authentication Modules) is a system security tool that allows system administrators to set authentication policy without having to recompile programs that handle authentication. Security Fix(es): A flaw was found in pam_access, where certain rules in its configuration file are mistakenly treated as hostnames. This vulnerability allows attackers to trick the system by pretending to be a trusted...

Suggestion

To upgrade the affected software

Reference:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-10041

CVE ID	CVSS Value	Attack Ve...	Impact	Vulnerability Details	Suggestion
CVE-2024-10963: Linux Pam_...	7.4	CVS...	Sensitive Inf	A flaw was found in pam_acce...	Official Fixes: 1. Repair Steps:...
CVE-2024-10041: Linux-Pam ...	4.7	CVS...	Sensitive Inf	A vulnerability was found in PA...	Official Fixes: In response to th...

Total Records: 2

Click a vulnerability notice name to go to the vulnerability details page. You can view the notice details, CVE details, suggestions, and affected assets. You can fix the vulnerabilities based on the suggestions.

- **Application vulnerabilities**

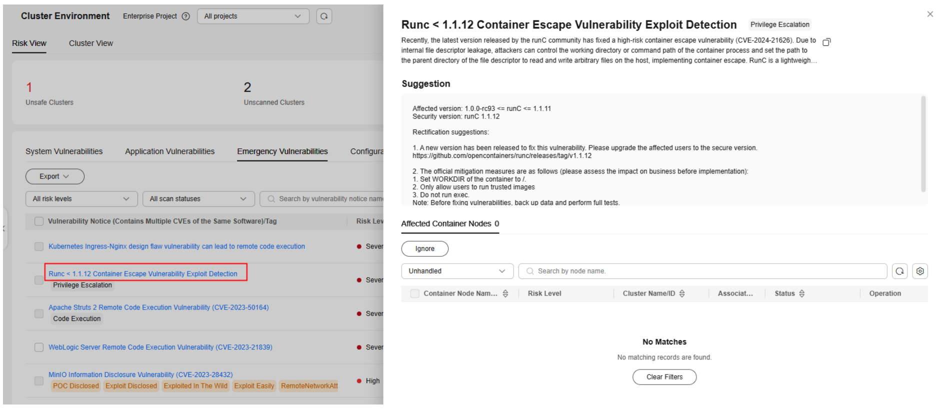
  Application software vulnerability scan results.

  Click a vulnerability notice name to go to the vulnerability details page. You can view the notice details, suggestions, and affected assets. You can fix the vulnerabilities based on the suggestions.

- **Emergency vulnerabilities**

  The emergency vulnerability list shows all the vulnerabilities of this type that can be detected by HSS.

Figure 5-80 Emergency vulnerabilities



Vulnerability Notice (Contains Multiple CVEs of the Same Software)/Tag	Risk Lev
Kubernetes Ingress-Nginx design flaw vulnerability can lead to remote code execution	● Sever
Runc < 1.1.12 Container Escape Vulnerability Exploit Detection Privilege Escalation	● Sever
Apache Struts 2 Remote Code Execution Vulnerability (CVE-2023-50164) Code Execution	● Sever
WebLogic Server Remote Code Execution Vulnerability (CVE-2023-21839)	● Sever
MinIO Information Disclosure Vulnerability (CVE-2023-28432) POC Disclosed Exploit Disclosed Exploited In The Wild Exploit Easily RemoteNetworkAtt	● High

Runc < 1.1.12 Container Escape Vulnerability Exploit Detection Privilege Escalation

Recently, the latest version released by the runC community has fixed a high-risk container escape vulnerability (CVE-2024-21626). Due to internal file descriptor leakage, attackers can control the working directory or command path of the container process and set the path to the parent directory of the file descriptor to read and write arbitrary files on the host, implementing container escape. RunC is a lightweigh...

Suggestion

Affected version: 1.0.0-rc93 <= runC <= 1.1.11
Security version: runC 1.1.12

Rectification suggestions:

1. A new version has been released to fix this vulnerability. Please upgrade the affected users to the secure version.
https://github.com/opencontainers/runc/releases/tag/v1.1.12

2. The official mitigation measures are as follows (please assess the impact on business before implementation):
1. Set WORKDIR of the container to /.
2. Only allow users to run trusted images
3. Do not run exec.
Note: Before fixing vulnerabilities, back up data and perform full tests.

Container Node Nam...	Risk Level	Cluster Name/ID	Associat...	Status	Operation

No Matches

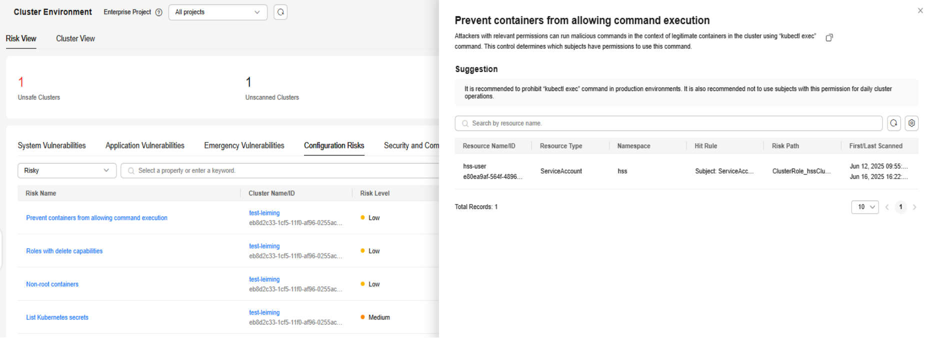
No matching records are found.

If the value of **Affected Containers/Container Nodes** is not 0 for an emergency vulnerability, there are containers or container nodes having emergency vulnerabilities. Click a vulnerability notice name to go to the details page. View the notice details, suggestions, and affected assets. You can fix the vulnerabilities based on the suggestions.

- **Configuration risks**

  The configuration risk list shows all the configuration risks that can be detected by HSS.

Figure 5-81 Configuration risks



Cluster Environment Enterprise Project All projects

Risk View Cluster View

1 Unsafe Clusters

1 Unscanned Clusters

System Vulnerabilities Application Vulnerabilities Emergency Vulnerabilities Configuration Risks Security and Com

Risky Select a property or enter a keyword.

Risk Name	Cluster Name/ID	Risk Level
Prevent containers from allowing command execution	test-leiming eb8d2c33-1cf5-11f0-af96-0255ac...	● Low
Roles with delete capabilities	test-leiming eb8d2c33-1cf5-11f0-af96-0255ac...	● Low
Non-root containers	test-leiming eb8d2c33-1cf5-11f0-af96-0255ac...	● Low
List Kubernetes secrets	test-leiming eb8d2c33-1cf5-11f0-af96-0255ac...	● Medium

Prevent containers from allowing command execution

Attackers with relevant permissions can run malicious commands in the context of legitimate containers in the cluster using "kubectl exec" command. This control determines which subjects have permissions to use this command.

Suggestion

It is recommended to prohibit "kubectl exec" command in production environments. It is also recommended not to use subjects with this permission for daily cluster operations.

Search by resource name.

Resource Name/ID	Resource Type	Namespace	Hit Rule	Risk Path	First/Last Scanned
hss-user e80ea9af-564f-4896...	ServiceAccount	hss	Subject: ServiceAcc...	ClusterRole_hssClu...	Jun 12, 2025 09:55:... Jun 16, 2025 16:22:...

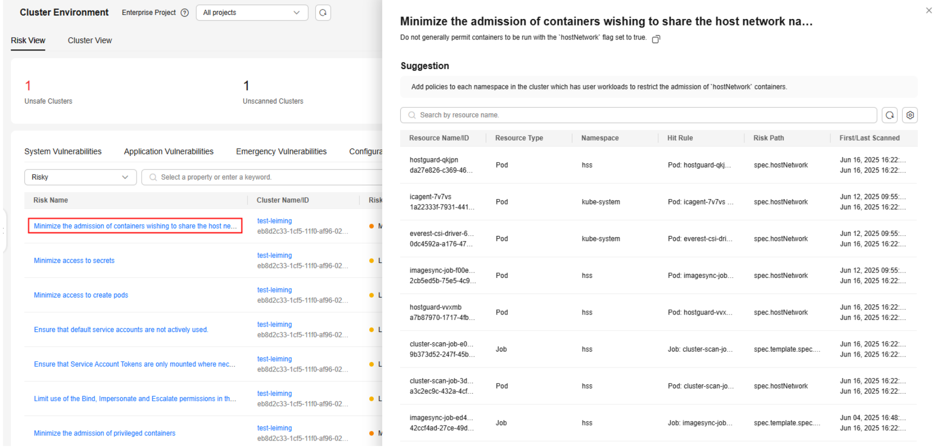
Total Records: 1 10 1

If the value of **Affected Resources** is not 0 for a configuration risk, there are Kubernetes resources having risks. Click a risk name. On the risk details page, view the suggestion and the information about affected resources, such as the resource names, namespaces, hit rules, and paths. You can rectify the configuration risks based on the information.

- **Security and compliance**

  The security and compliance list shows all the issues of this type that can be detected by HSS.

Figure 5-82 Security and compliance



Cluster Environment Enterprise Project All projects

Risk View Cluster View

1 Unsafe Clusters

1 Unscanned Clusters

System Vulnerabilities Application Vulnerabilities Emergency Vulnerabilities Configura

Risky Select a property or enter a keyword.

Risk Name	Cluster Name/ID	Risk
Minimize the admission of containers wishing to share the host ne...	test-leiming eb8d2c33-1cf5-11f0-af96-02...	● M
Minimize access to secrets	test-leiming eb8d2c33-1cf5-11f0-af96-02...	● L
Minimize access to create pods	test-leiming eb8d2c33-1cf5-11f0-af96-02...	● L
Ensure that default service accounts are not actively used.	test-leiming eb8d2c33-1cf5-11f0-af96-02...	● L
Ensure that Service Account Tokens are only mounted where nec...	test-leiming eb8d2c33-1cf5-11f0-af96-02...	● L
Limit use of the Bind, Impersonate and Escalate permissions in th...	test-leiming eb8d2c33-1cf5-11f0-af96-02...	● L
Minimize the admission of privileged containers	test-leiming eb8d2c33-1cf5-11f0-af96-02...	● M

Minimize the admission of containers wishing to share the host network na...

Do not generally permit containers to be run with the `hostNetwork` flag set to true.

Suggestion

Add policies to each namespace in the cluster which has user workloads to restrict the admission of `hostNetwork` containers.

Search by resource name.

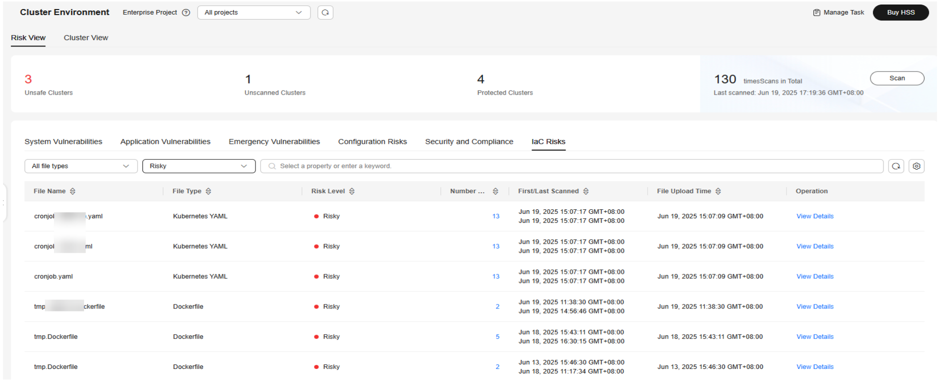
Resource Name/ID	Resource Type	Namespace	Hit Rule	Risk Path	First/Last Scanned
hostguard-qkjpn da27e826-c369-46...	Pod	hss	Pod: hostguard-qkj...	spec.hostNetwork	Jun 16, 2025 16:22:... Jun 16, 2025 16:22:...
icagent-7v7vs 1a22333f-7931-441...	Pod	kube-system	Pod: icagent-7v7vs ...	spec.hostNetwork	Jun 12, 2025 09:55:... Jun 16, 2025 16:22:...
everest-csi-driver-6... 0dc4592a-a176-47...	Pod	kube-system	Pod: everest-csi-dri...	spec.hostNetwork	Jun 12, 2025 09:55:... Jun 16, 2025 16:22:...
imagesync-job-f00e... 2cb5ed5b-75e5-4c9...	Pod	hss	Pod: imagesync-job...	spec.hostNetwork	Jun 12, 2025 09:55:... Jun 16, 2025 16:22:...
hostguard-vvxmb a7b87970-1717-4fb...	Pod	hss	Pod: hostguard-vvx...	spec.hostNetwork	Jun 16, 2025 16:22:... Jun 16, 2025 16:22:...
cluster-scan-job-e0... 9b373d52-247f-45b...	Job	hss	Job: cluster-scan-jo...	spec.template.spec....	Jun 16, 2025 16:22:... Jun 16, 2025 16:22:...
cluster-scan-job-3d... a3c2ec9c-432a-4cf...	Pod	hss	Pod: cluster-scan-jo...	spec.hostNetwork	Jun 16, 2025 16:22:... Jun 16, 2025 16:22:...
imagesync-job-ed4... 42ccf4ad-27ce-49d...	Job	hss	Job: imagesync-job...	spec.template.spec....	Jun 04, 2025 16:48:... Jun 16, 2025 16:22:...

If the value of **Affected Resources** is not 0 for a security and compliance issue, there are Kubernetes resources having risks. Click a risk name. On the risk details page, view the suggestion and the information about affected resources, such as the resource names, namespaces, hit rules, and paths. You can rectify the security and compliance issue based on the information.

- IaC risks

  IaC scan results.

Figure 5-83 IaC risks



3 Unsafe Clusters

1 Unscanned Clusters

4 Protected Clusters

130 timesScans in Total
Last scanned: Jun 19, 2025 17:19:36 GMT+08:00

File Name	File Type	Risk Level	Number ...	First/Last Scanned	File Upload Time	Operation
cronjol[redacted].yaml	Kubernetes YAML	● Risky	13	Jun 19, 2025 15:07:17 GMT+08:00 Jun 19, 2025 15:07:17 GMT+08:00	Jun 19, 2025 15:07:09 GMT+08:00	View Details
cronjol[redacted]ml	Kubernetes YAML	● Risky	13	Jun 19, 2025 15:07:17 GMT+08:00 Jun 19, 2025 15:07:17 GMT+08:00	Jun 19, 2025 15:07:09 GMT+08:00	View Details
cronjob.yaml	Kubernetes YAML	● Risky	13	Jun 19, 2025 15:07:17 GMT+08:00 Jun 19, 2025 15:07:17 GMT+08:00	Jun 19, 2025 15:07:09 GMT+08:00	View Details
tmp[redacted]ckerfile	Dockerfile	● Risky	2	Jun 19, 2025 11:38:30 GMT+08:00 Jun 19, 2025 14:56:46 GMT+08:00	Jun 19, 2025 11:38:30 GMT+08:00	View Details
tmp.Dockerfile	Dockerfile	● Risky	5	Jun 18, 2025 15:43:11 GMT+08:00 Jun 18, 2025 16:30:15 GMT+08:00	Jun 18, 2025 15:43:11 GMT+08:00	View Details
tmp.Dockerfile	Dockerfile	● Risky	2	Jun 13, 2025 15:46:30 GMT+08:00 Jun 18, 2025 11:17:34 GMT+08:00	Jun 13, 2025 15:46:30 GMT+08:00	View Details

If **Risky** is displayed in the **Risk Level** column of a file, the file is insecure. You can perform the following operations to view and handle the risks:

a. Click **View Details** in the **Operation** column. On the details page, view the risks, description, and suggestions.

b. Click a risk name. On the risk details page that is displayed, view the risk hit rule, risk path, and affected resources.

c. Manually rectify the risks based on the information provided.

----End

Viewing and Handling Cluster Environment Risks in the Cluster View

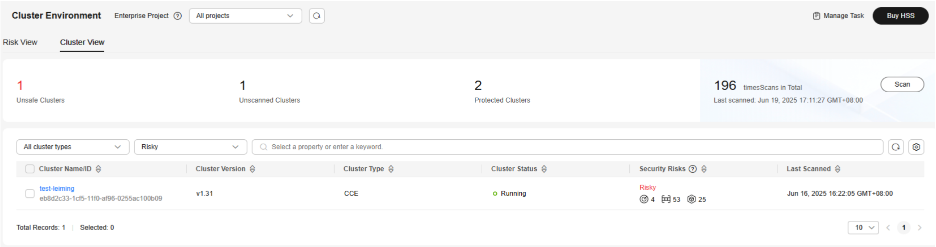
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Risk Management** > **Cluster Environment**.

Step 4 Click **Cluster View**.

Figure 5-84 Cluster view



1 Unsafe Clusters

1 Unscanned Clusters

2 Protected Clusters

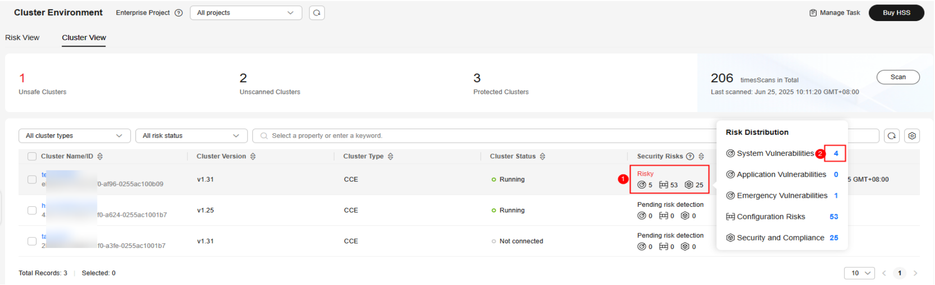
196 timesScans in Total
Last scanned: Jun 19, 2025 17:11:27 GMT+08:00

□	Cluster Name/ID	Cluster Version	Cluster Type	Cluster Status	Security Risks	Last Scanned
□	test-leiming eb8d2c33-1cf5-11f0-af96-0255ac100b09	v1.31	CCE	○ Running	Risky 4 53 25	Jun 16, 2025 16:22:05 GMT+08:00

Total Records: 1 | Selected: 0

Step 5 If **Risky** is displayed in the **Security Risks** column of a cluster, hover the cursor over the cell to view the risk distribution. Click the number of a risk to go to the cluster risk details page.

Figure 5-85 Risk distribution



1 Unsafe Clusters | 2 Unscanned Clusters | 3 Protected Clusters | 206 timesScans in Total

Last scanned: Jun 25, 2025 10:11:20 GMT+08:00

Cluster Name/ID	Cluster Version	Cluster Type	Cluster Status	Security Risks
[redacted]0-af96-0255ac100b09	v1.31	CCE	Running	Risky 5 53 25
[redacted]f0-a624-0255ac1001b7	v1.25	CCE	Running	Pending risk detection 0 0 0
[redacted]f0-a3fe-0255ac1001b7	v1.31	CCE	Not connected	Pending risk detection 0 0 0

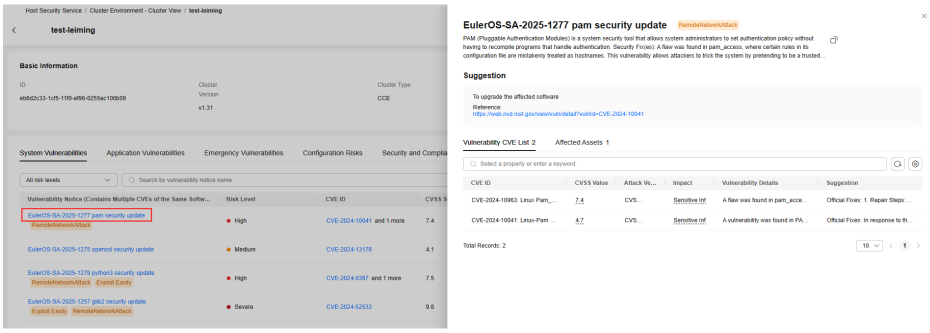
Total Records: 3 | Selected: 0

Step 6 View and handle risks. They include:

- **System vulnerabilities**

  OS vulnerability scan results.

  Figure 5-86 System vulnerabilities

  
  Host Security Service / Cluster Environment - Cluster View / test-leiming
test-leiming
System Vulnerabilities
Application Vulnerabilities
Emergency Vulnerabilities
Configuration Risks
Security and Complia
All risk levels
Search by vulnerability notice name.
Vulnerability CVE List 2
Affected Assets 1
Select a property or enter a keyword.
10
1

  Basic Information

  ID: eb8d2c33-1cf5-11f0-af96-0255ac100b09 | Cluster Version: v1.31 | Cluster Type: CCE

Vulnerability Notice (Contains Multiple CVEs of the Same Softw...	Risk Level	CVE ID	CVSS S
EulerOS-SA-2025-1277 pam security update RemoteNetworkAttack	High	CVE-2024-10041 and 1 more	7.4
EulerOS-SA-2025-1275 openssl security update	Medium	CVE-2024-13176	4.1
EulerOS-SA-2025-1279 python3 security update RemoteNetworkAttack Exploit Easily	High	CVE-2024-0397 and 1 more	7.5
EulerOS-SA-2025-1257 glib2 security update Exploit Easily RemoteNetworkAttack	Severe	CVE-2024-52533	9.8

  EulerOS-SA-2025-1277 pam security update RemoteNetworkAttack

  PAM (Pluggable Authentication Modules) is a system security tool that allows system administrators to set authentication policy without having to recompile programs that handle authentication. Security Fix(es): A flaw was found in pam_access, where certain rules in its configuration file are mistakenly treated as hostnames. This vulnerability allows attackers to trick the system by pretending to be a trusted...

  Suggestion

  To upgrade the affected software

  Reference:
  https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-10041

CVE ID	CVSS Value	Attack Ve...	Impact	Vulnerability Details	Suggestion
CVE-2024-10963: Linux Pam_...	7.4	CVS...	Sensitive Inf	A flaw was found in pam_acce...	Official Fixes: 1. Repair Steps:...
CVE-2024-10041: Linux-Pam ...	4.7	CVS...	Sensitive Inf	A vulnerability was found in PA...	Official Fixes: In response to th...

  Total Records: 2

  Click a vulnerability notice name to go to the vulnerability details page. You can view the notice details, CVE details, suggestions, and affected assets. You can fix the vulnerabilities based on the suggestions.

- **Application vulnerabilities**

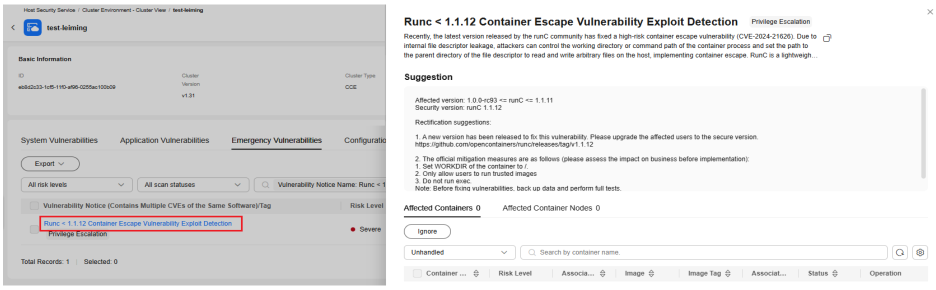
  Application software vulnerability scan results.

  Click a vulnerability notice name to go to the vulnerability details page. You can view the notice details, suggestions, and affected assets. You can fix the vulnerabilities based on the suggestions.

- **Emergency vulnerabilities**

  The emergency vulnerability list shows the emergency vulnerabilities of container assets.

  Figure 5-87 Emergency vulnerabilities

  
  Host Security Service / Cluster Environment - Cluster View / test-leiming
test-leiming
System Vulnerabilities
Application Vulnerabilities
Emergency Vulnerabilities
Configuratio
Export
All risk levels
All scan statuses
Affected Containers 0
Affected Container Nodes 0
Ignore
Unhandled
Search by container name.

  Basic Information

  ID: eb8d2c33-1cf5-11f0-af96-0255ac100b09 | Cluster Version: v1.31 | Cluster Type: CCE

  Vulnerability Notice Name: Runc < 1

Vulnerability Notice (Contains Multiple CVEs of the Same Software)/Tag	Risk Level
Runc < 1.1.12 Container Escape Vulnerability Exploit Detection Privilege Escalation	Severe

  Total Records: 1 | Selected: 0

  Runc < 1.1.12 Container Escape Vulnerability Exploit Detection Privilege Escalation

  Recently, the latest version released by the runC community has fixed a high-risk container escape vulnerability (CVE-2024-21626). Due to internal file descriptor leakage, attackers can control the working directory or command path of the container process and set the path to the parent directory of the file descriptor to read and write arbitrary files on the host, implementing container escape. RunC is a lightweigh...

  Suggestion

  Affected version: 1.0.0-rc93 <= runC <= 1.1.11
  Security version: runC 1.1.12

  Rectification suggestions:

  1. A new version has been released to fix this vulnerability. Please upgrade the affected users to the secure version.
  https://github.com/opencontainers/runc/releases/tag/v1.1.12

  2. The official mitigation measures are as follows (please assess the impact on business before implementation):
  1. Set WORKDIR of the container to /.
  2. Only allow users to run trusted images
  3. Do not run exec.
  Note: Before fixing vulnerabilities, back up data and perform full tests.

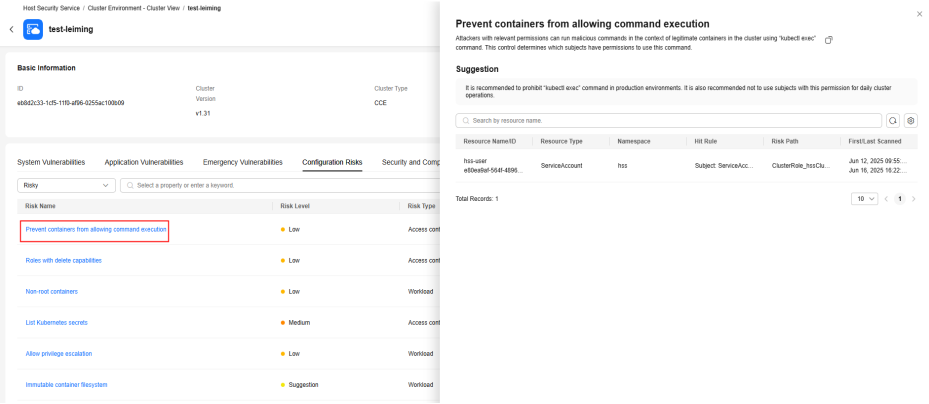
Container ...	Risk Level	Associa...	Image	Image Tag	Associat...	Status	Operation

Click a vulnerability notice name to go to the details page. View the notice details, suggestions, and affected assets. You can fix the vulnerabilities based on the suggestions.

- **Configuration risks**

  The configuration risk list shows all the configuration risks that can be detected by HSS.

Figure 5-88 Configuration risks


Host Security Service / Cluster Environment - Cluster View / test-leiming
test-leiming
System Vulnerabilities
Application Vulnerabilities
Emergency Vulnerabilities
Configuration Risks
Security and Comp
Select a property or enter a keyword.
Search by resource name.

Basic Information

ID: eb8d2c33-1cf5-11f0-af96-0255ac100b09

Cluster Version: v1.31

Cluster Type: CCE

Risky

Risk Name	Risk Level	Risk Type
Prevent containers from allowing command execution	Low	Access cont
Roles with delete capabilities	Low	Access cont
Non-root containers	Low	Workload
List Kubernetes secrets	Medium	Access cont
Allow privilege escalation	Low	Workload
Immutable container filesystem	Suggestion	Workload

Prevent containers from allowing command execution

Attackers with relevant permissions can run malicious commands in the context of legitimate containers in the cluster using "kubectl exec" command. This control determines which subjects have permissions to use this command.

Suggestion

It is recommended to prohibit "kubectl exec" command in production environments. It is also recommended not to use subjects with this permission for daily cluster operations.

Resource Name/ID	Resource Type	Namespace	Hit Rule	Risk Path	First/Last Scanned
hss-user e80ea9af-564f-4896...	ServiceAccount	hss	Subject: ServiceAcc...	ClusterRole_hssClu...	Jun 12, 2025 09:55:... Jun 16, 2025 16:22:...

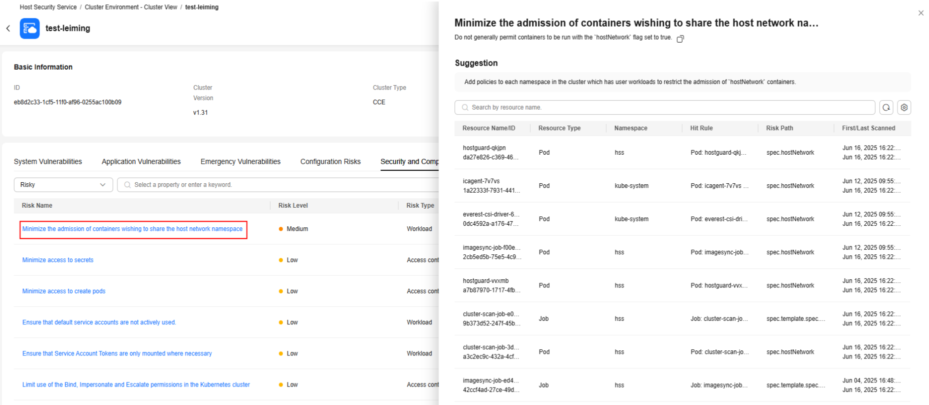
Total Records: 1 10 1

If the value of **Affected Resources** is not 0 for a configuration risk, there are Kubernetes resources having risks. Click a risk name. On the risk details page, view the suggestion and the information about affected resources, such as the resource names, namespaces, hit rules, and paths. You can rectify the configuration risks based on the information.

- **Security and compliance**

  The security and compliance list shows all the issues of this type that can be detected by HSS.

Figure 5-89 Security and compliance


Host Security Service / Cluster Environment - Cluster View / test-leiming
test-leiming
System Vulnerabilities
Application Vulnerabilities
Emergency Vulnerabilities
Configuration Risks
Security and Comp
Select a property or enter a keyword.
Search by resource name.

Basic Information

ID: eb8d2c33-1cf5-11f0-af96-0255ac100b09

Cluster Version: v1.31

Cluster Type: CCE

Risky

Risk Name	Risk Level	Risk Type
Minimize the admission of containers wishing to share the host network namespace	Medium	Workload
Minimize access to secrets	Low	Access cont
Minimize access to create pods	Low	Access cont
Ensure that default service accounts are not actively used.	Low	Workload
Ensure that Service Account Tokens are only mounted where necessary	Low	Workload
Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster	Low	Access cont

Minimize the admission of containers wishing to share the host network na...

Do not generally permit containers to be run with the `hostNetwork` flag set to true.

Suggestion

Add policies to each namespace in the cluster which has user workloads to restrict the admission of `hostNetwork` containers.

Resource Name/ID	Resource Type	Namespace	Hit Rule	Risk Path	First/Last Scanned
hostguard-qkjpn da27e826-c369-46...	Pod	hss	Pod: hostguard-qkj...	spec.hostNetwork	Jun 16, 2025 16:22:... Jun 16, 2025 16:22:...
icagent-7v7vs 1a22333f-7931-441...	Pod	kube-system	Pod: icagent-7v7vs ...	spec.hostNetwork	Jun 12, 2025 09:55:... Jun 16, 2025 16:22:...
everest-csi-driver-6... 0dc4592a-a176-47...	Pod	kube-system	Pod: everest-csi-dri...	spec.hostNetwork	Jun 12, 2025 09:55:... Jun 16, 2025 16:22:...
imagesync-job-f00e... 2cb5ed5b-75e5-4c9...	Pod	hss	Pod: imagesync-job...	spec.hostNetwork	Jun 12, 2025 09:55:... Jun 16, 2025 16:22:...
hostguard-vvxmb a7b87970-1717-4fb...	Pod	hss	Pod: hostguard-vvx...	spec.hostNetwork	Jun 16, 2025 16:22:... Jun 16, 2025 16:22:...
cluster-scan-job-e0... 9b373d52-247f-45b...	Job	hss	Job: cluster-scan-jo...	spec.template.spec....	Jun 16, 2025 16:22:... Jun 16, 2025 16:22:...
cluster-scan-job-3d... a3c2ec9c-432a-4cf...	Pod	hss	Pod: cluster-scan-jo...	spec.hostNetwork	Jun 16, 2025 16:22:... Jun 16, 2025 16:22:...
imagesync-job-ed4... 42ccf4ad-27ce-49d...	Job	hss	Job: imagesync-job...	spec.template.spec....	Jun 04, 2025 16:48:... Jun 16, 2025 16:22:...

If the value of **Affected Resources** is not 0 for a security and compliance issue, there are Kubernetes resources having risks. Click a risk name. On the risk details page, view the suggestion and the information about affected resources, such as the resource names, namespaces, hit rules, and paths. You can rectify the security and compliance issue based on the information.

----End

6 Server Protection

6.1 Application Protection

6.1.1 Application Protection Overview

Based on runtime application self-protection (RASP), the application protection feature provides security check and protection for running applications. You do not need to modify application files. You simply need to inject probes to applications to enjoy powerful security protection capabilities.

Technical Principles

Probes (monitoring and protection code) are added to the checkpoints (key functions) of applications through dynamic code injection. The probes identify attacks based on predefined rules, data passing through the checkpoints, and contexts (application logic, configurations, data, and event flows).

Detection Capabilities

Table 6-1 describes the types of attacks that can be detected by application protection.

Table 6-1 Attack types detected by application protection

Attack Type	Description	Rule Name	Detection
SQL injection	SQL injection is an attack technology. Attackers exploit the vulnerabilities of dynamic SQL query in web applications to insert malicious code into user input fields and trick the database into executing SQL commands to steal, tamper with, or damage sensitive data, or run dangerous system-level commands on the database server. Most websites and web applications need to use SQL databases. Therefore, SQL injection attacks become one of the oldest and most widely launched network attacks.	SQLI	Detect and defend against SQL injection attacks, and check web applications for related vulnerabilities.
OS command injection	OS command injection is a web program vulnerability that is usually found in applications that require user input. If there is no effective filtering and verification mechanism for user input, this vulnerability may be exploited. It allows attackers to execute arbitrary OS commands on the server where an application is running.	CMDI	Detect and defend against remote OS command injection attacks and check web applications for related vulnerabilities.
XSS	Cross-site scripting (XSS) is a typical web program vulnerability exploit attack. Attackers can inject executable malicious scripts into websites or web applications where web programs do not check user input. When users access web pages, the malicious scripts are executed to steal users' personal data, display advertisements, or even tamper with web page content.	XSS	Detect and defend against stored XSS attacks.

Attack Type	Description	Rule Name	Detection
Log4j RCE vulnerability	Log4j RCE is a major security vulnerability in Apache Log4j 2.x. This vulnerability allows attackers to inject and execute remote code through Java Naming and Directory Interface (JNDI).	Log4jRCE	Detect and defend against remote code execution and intercept attacks.
Web shell upload	Uploading web shells is a network attack method. Attackers upload malicious code such as web shells to a server through vulnerability exploit or other methods to obtain the control permission for the server.	WebShellUpload	Detect and defend against attacks that upload dangerous files, change file names, or change file name extension types; and check web applications for related vulnerabilities.
Memory injection	Memory injection is an advanced network attack technology. Attackers inject malicious code into the memory, bypassing the traditional security defense mechanism and controlling the target system.	FilelessWebshell	Detect and defend against memory injection attacks.
XXE	XXE refers to the XML External Entity Injection vulnerability. If external entity reference is not disabled when an application parses XML files, attackers can construct malicious XML content to read arbitrary files and execute system commands.	XXE	Detect and defend against XXE injection attacks, and check web applications for related vulnerabilities.
Deserialization input	Deserialization is a process of restoring serialized data (such as strings and byte streams) to original objects. In the process of generating a deserialized object, an attacker may construct specific serialized data input to control the generated object and launch attacks.	UntrustedDeserialization	Detect deserialization attacks that exploit unsafe classes.

Attack Type	Description	Rule Name	Detection
File directory traversal	File directory traversal means that an attacker accesses or reads any file or folder on a server by modifying URLs or using special characters to bypass the security check of an application.	FileDirAccess	Check whether sensitive directories or files are accessed.
Struts2 OGNL	Struts2 OGNL refers to the Object-Graph Navigation Language (OGNL) in Struts2 in the Java web framework. If OGNL expressions are externally controllable, attackers can construct malicious OGNL expressions to make programs perform malicious operations.	Struts2OGNL	Detect OGNL code execution.
Command execution using JSP	Java Server Pages (JSP) is a technology for developing dynamic web pages. Attackers may exploit JSP security vulnerabilities to execute invalid OS commands, causing data leakage and service interruption.	SuspiciousBehavior	Detect command execution using JSP.
File deletion using JSP	Attackers may exploit JSP security vulnerabilities to delete files from a server.	SuspiciousBehavior	Detect file deletion using JSP.
Database connection exception	Database connection exceptions include but are not limited to network exceptions, configuration errors, and permission exceptions. These exceptions may indicate that applications are being attacked.	SuspiciousException	Detect authentication and communication exceptions thrown by database connections.

Attack Type	Description	Rule Name	Detection
0-day vulnerability	0-day vulnerabilities, also called zero-day attacks, usually refers to security vulnerabilities that have not been patched. If such vulnerabilities are detected, hackers can exploit these vulnerabilities to launch zero-day attacks.	● zeroDay ● zeroDayDetect	● Check whether the stack hash of a command is in the whitelist of the web application. ● Detect and defend against expression injection attacks, and check web applications for related vulnerabilities.
SecurityManager permission exception	SecurityManager is a Java security manager class that manages and controls the security of applications. When the SecurityManager detects that the code performs an operation that is not allowed, an exception is thrown.	SuspiciousException	Detect exceptions thrown by SecurityManager.
JNDI injection	When an application uses the lookup method of JNDI, if the queried URL can be controlled externally, an attacker can construct a malicious URL to make the server load malicious payloads and implement remote code execution.	JNDI	Detect and defend against JNDI injection attacks, and check web applications for related vulnerabilities.
Expression injection	Expression Language (EL) injection. If EL expressions are externally controllable, attackers can construct malicious EL expressions to make programs perform malicious operations.	ExpressionInject	Detect and defend against expression injection attacks, and check web applications for related vulnerabilities.

Application Scenarios and Advantages

- Context awareness: Application protection can provide accurate detection results based on application context.

- Complementary with WAF: Application protection can detect the data written in the memory and unauthorized database access when applications are running.
- 0-day vulnerability defense: Application protection can dynamically detect and defend against attacks in real time when applications are running, blocking 0-day vulnerability exploits.

Constraints

- Application protection is available in HSS premium, WTP, and container editions. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.
- Application protection can only protect web applications that meet the following conditions:
  - JDK: JDK 8, JDK 11, JDK 17
  - Web applications:
    - Windows (64-bit): Tomcat
    - Linux (64-bit): Tomcat, WebLogic, Netty, and Jetty

    The version requirements are as follows:
    - Tomcat 7.0.55 or later
    - WebLogic 12C or later
    - Netty 4.1.0.Final or later
    - Jetty 9.3.19 or later
- Containers that meet the following conditions can use container application protection:
  - Kubernetes 1.19 or later
  - Docker 18 or later

Process of Using Application Protection

Figure 6-1 Usage process

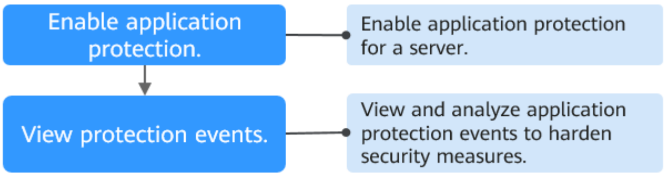

Enable application protection.
Enable application protection for a server.
View protection events.
View and analyze application protection events to harden security measures.

Table 6-2 Process description

Operation	Description
Enabling Application Protection	Enable application protection for a server to assess application security in real time.

Operation	Description
Viewing Application Protection Events	Analyze triggered events, harden application protection measures, and improve application security.

6.1.2 Enabling Application Protection

Scenario

To protect web applications, enable application protection for servers. While protection is enabled, the microservice RASP plug-ins are installed on servers.

How to Enable

Application protection can be enabled automatically or manually. The differences are as follows:

How to Enable	Advantage	Restriction	Operation
Automatically	• You do not need to manually configure application protection startup parameters. • HSS automatically identifies and accesses web applications that have listening ports on the protected servers, and dynamically loads or unloads application protection as needed when web applications are running.	• This method depends on **automatic dynamic RASP**, which is in the OBT phase. To use this function, **submit a service ticket**. • If a web application is just started and runs for 5 minutes or less, RASP cannot be enabled using this method. When the running time of the application exceeds 5 minutes, RASP is automatically enabled. • Web applications of JRE 8, JRE 11, and JRE 17 are not supported. • For JDK 17, **--add-opens=java.base/java.lang=ALL-UNNAMED** needs to be added to the web application startup parameters.	**Automatically Enabling Application Protection**

How to Enable	Advantage	Restriction	Operation
Manually	● Web applications without listening ports can be accessed. ● Web applications of JRE 8, JRE 11, and JRE 17 are supported.	You need to manually configure application protection startup parameters for applications.	**Manually Enabling Application Protection**

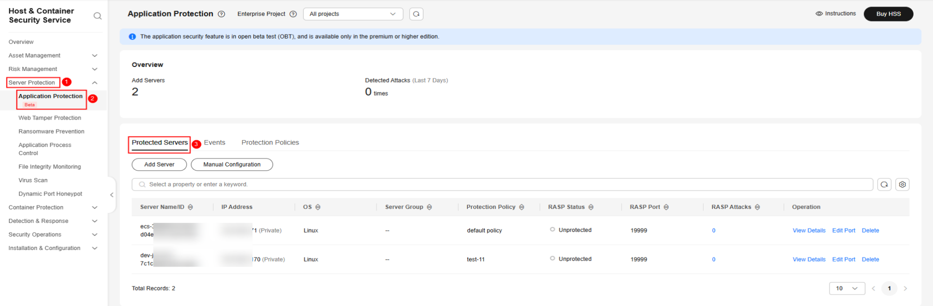
Automatically Enabling Application Protection

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Application Protection**. Click the **Protected Servers** tab.

Figure 6-2 Viewing protection settings



The application security feature is in open beta test (OBT), and is available only in the premium or higher edition.

Overview

Add Servers 2

Detected Attacks (Last 7 Days) 0 times

Server Name/ID	IP Address	OS	Server Group	Protection Policy	RASP Status	RASP Port	RASP Attacks	Operation
ecs-[redacted] d04e[redacted]	[redacted]1 (Private)	Linux	--	default policy	○ Unprotected	19999	0	View Details Edit Port Delete
dev-[redacted] 7c1c[redacted]	[redacted]70 (Private)	Linux	--	test-11	○ Unprotected	19999	0	View Details Edit Port Delete

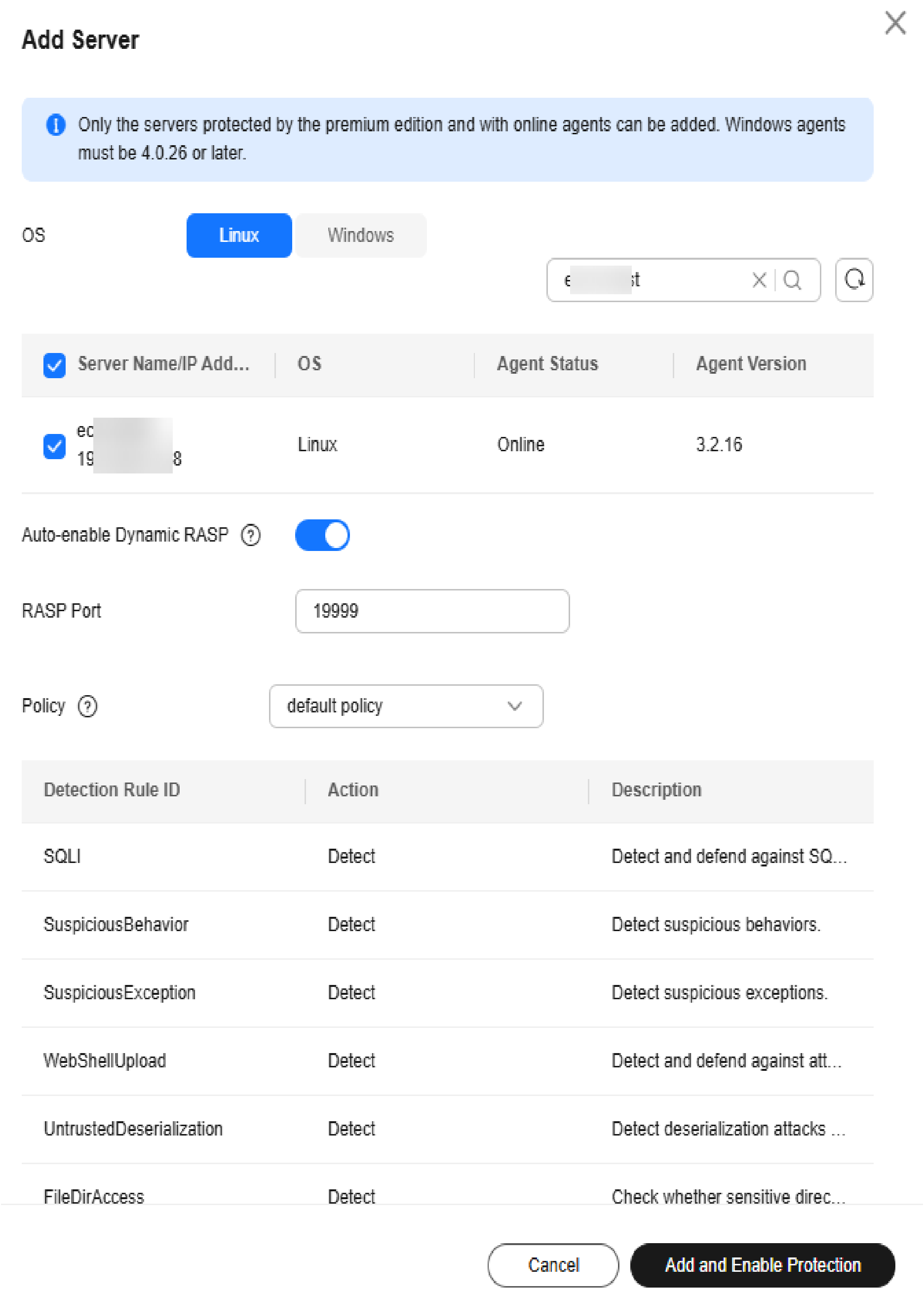
Total Records: 2

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click **Add Server**. The **Add Server** slide-out panel is displayed.

Step 6 Select servers and a protection policy. Click **Add and Enable Protection**. For more information, see **Table 6-3**.

Figure 6-3 Adding protected servers



Add Server

Only the servers protected by the premium edition and with online agents can be added. Windows agents must be 4.0.26 or later.

OS: Linux | Windows

e[redacted]t

☑ Server Name/IP Add...	OS	Agent Status	Agent Version
☑ ec[redacted] 19[redacted]8	Linux	Online	3.2.16

Auto-enable Dynamic RASP: ●

RASP Port: 19999

Policy: default policy

Detection Rule ID	Action	Description
SQLI	Detect	Detect and defend against SQ...
SuspiciousBehavior	Detect	Detect suspicious behaviors.
SuspiciousException	Detect	Detect suspicious exceptions.
WebShellUpload	Detect	Detect and defend against att...
UntrustedDeserialization	Detect	Detect deserialization attacks ...
FileDirAccess	Detect	Check whether sensitive direc...

Table 6-3 Parameters for adding a protected server

Parameter	Description	Example Value
OS	Server OS type. It can be Linux or Windows.	**Linux**

Parameter	Description	Example Value
Auto-enable Dynamic RASP	Whether to automatically enable dynamic RASP. If this function is enabled, JVM Attach capabilities are used to automatically identify and access web applications (including container environments) that have listening ports on servers, and to integrate application protection into the web applications. In this way, application protection can be dynamically loaded and unloaded when web applications are running. The web applications do not need to be restarted, thereby ensuring service continuity. If a web application is just started and runs for 5 minutes or less, the function cannot be enabled using this method. When the running time of the application exceeds 5 minutes, the function is automatically enabled. **NOTE** This function is in the OBT phase. To use it, **submit a service ticket**.	**Enabled**
RASP Port	RASP listening port.	**19999**
Policy	Application protection policy. HSS provides a default policy, which contains all the detection rules of application protection. For details, see **Detection Capabilities**. If the default policy is not applicable to your workloads, you can create a custom policy. For details, see **Adding a Protection Policy**.	**default policy**

Step 7 On the **Protected Servers** page, check whether the **RASP Status** of the server is **Protected**. If yes, RASP has been enabled for all the web applications on the server.

- If the **RASP Status** of a server is **Enabling protection**, the system is installing the RASP plug-in and enabling RASP for the server. Wait for several minutes.
- If the **RASP Status** of a server is **Protection failed** or **Partially protected**, click **View Details** in the **Operation** column of the server to view the cause of the protection failure and rectify faults accordingly.

  If information similar to the following is displayed, go to **Step 8**.

```
11\u0502 27, 2024 11:15:26 \u024f\u03a7 com.huawei.hisec.secshield.main.AttachMain verify\r\n
\u044f\u0598: JDK 17 must contain parameter \"--add-opens=java.base/java.lang=ALL-UNNAMED\"\r
\n11\u0502 27, 2024 11:15:26 \u024f\u03a7 com.huawei.hisec.secshield.main.AttachMain verify\r\n
\u044f\u0598: JDK 17 must contain parameter \"--add-opens=java.base/java.lang=ALL-UNNAMED\"\r
\n
```

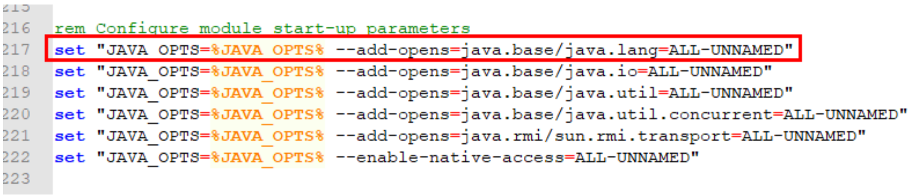
Step 8 (Optional) For a web application of JDK 17, add the **--add-opens=java.base/java.lang=ALL-UNNAMED** parameter to its startup script.

The configuration method varies depending on the application type and version. The following uses Apache Tomcat 11.0.0 as an example.

- Tomcat (Windows)

  Add the **--add-opens=java.base/java.lang=ALL-UNNAMED** parameter to the **catalina.bat** file in the bin directory of the Tomcat installation directory, as shown in **Figure 6-4**.

  Figure 6-4 catalina.bat

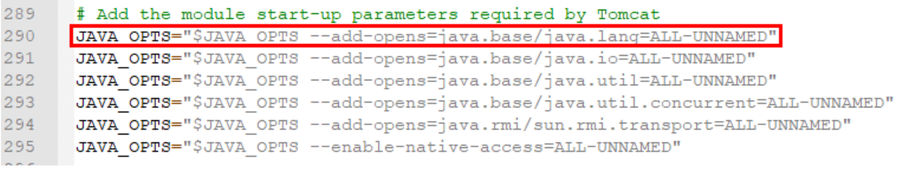
  

  ```
  rem Configure module start-up parameters
  set "JAVA_OPTS=%JAVA_OPTS% --add-opens=java.base/java.lang=ALL-UNNAMED"
  set "JAVA_OPTS=%JAVA_OPTS% --add-opens=java.base/java.io=ALL-UNNAMED"
  set "JAVA_OPTS=%JAVA_OPTS% --add-opens=java.base/java.util=ALL-UNNAMED"
  set "JAVA_OPTS=%JAVA_OPTS% --add-opens=java.base/java.util.concurrent=ALL-UNNAMED"
  set "JAVA_OPTS=%JAVA_OPTS% --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED"
  set "JAVA_OPTS=%JAVA_OPTS% --enable-native-access=ALL-UNNAMED"
  ```

- Tomcat (Linux)

  Add the **--add-opens=java.base/java.lang=ALL-UNNAMED** parameter to the **catalina.sh** file in the bin directory of the Tomcat installation directory, as shown in **Figure 6-5**.

  Figure 6-5 catalina.sh

  ```
  # Add the module start-up parameters required by Tomcat
  JAVA_OPTS="$JAVA_OPTS --add-opens=java.base/java.lang=ALL-UNNAMED"
  JAVA_OPTS="$JAVA_OPTS --add-opens=java.base/java.io=ALL-UNNAMED"
  JAVA_OPTS="$JAVA_OPTS --add-opens=java.base/java.util=ALL-UNNAMED"
  JAVA_OPTS="$JAVA_OPTS --add-opens=java.base/java.util.concurrent=ALL-UNNAMED"
  JAVA_OPTS="$JAVA_OPTS --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED"
  JAVA_OPTS="$JAVA_OPTS --enable-native-access=ALL-UNNAMED"
  ```

Wait for 5 to 10 minutes after the configuration is complete. If the **RASP Status** of the server is **Protected**, RASP has been enabled.

----End

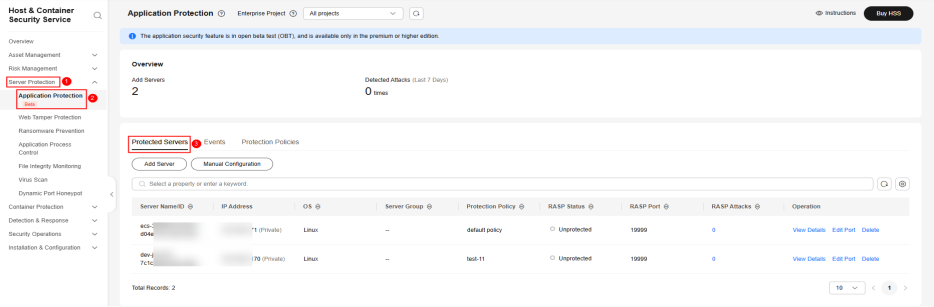
Manually Enabling Application Protection

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

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

Step 3 Choose **Server Protection** > **Application Protection**. Click the **Protected Servers** tab.

Figure 6-6 Viewing protection settings



The application security feature is in open beta test (OBT), and is available only in the premium or higher edition.

Overview

Add Servers
2

Detected Attacks (Last 7 Days)
0 times

Server Name/ID	IP Address	OS	Server Group	Protection Policy	RASP Status	RASP Port	RASP Attacks	Operation
ecs-[redacted] d04e	[redacted]1 (Private)	Linux	--	default policy	○ Unprotected	19999	0	View Details Edit Port Delete
dev-[redacted] 7c1c	[redacted]70 (Private)	Linux	--	test-11	○ Unprotected	19999	0	View Details Edit Port Delete

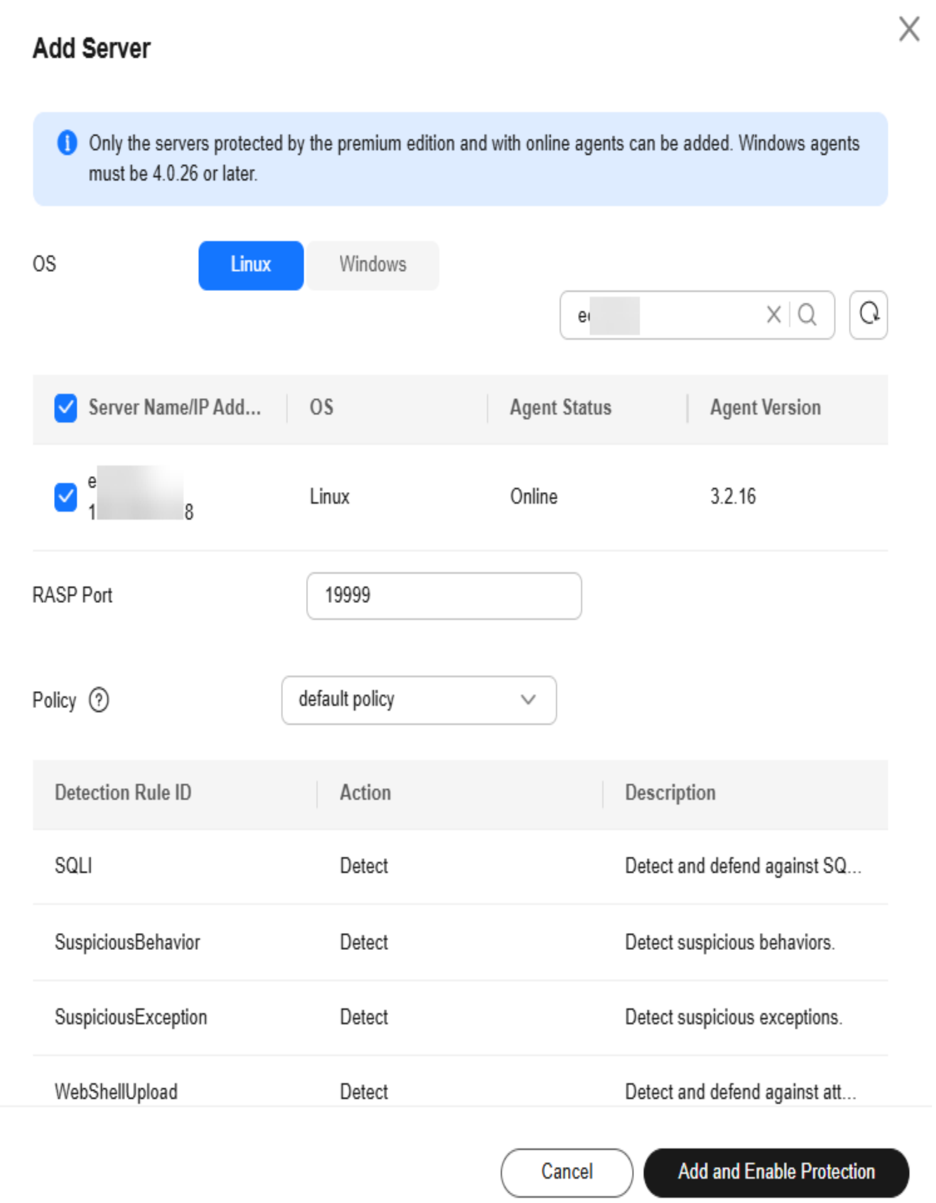
Total Records: 2

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click **Add Server**. The **Add Server** slide-out panel is displayed.

Step 6 Select servers and a protection policy. Click **Add and Enable Protection**. For more information, see **Table 6-4**.

Figure 6-7 Adding protected servers



Add Server

Only the servers protected by the premium edition and with online agents can be added. Windows agents must be 4.0.26 or later.

OS: Linux | Windows

e[redacted]

☑ Server Name/IP Add...	OS	Agent Status	Agent Version
☑ e[redacted] 1[redacted]8	Linux	Online	3.2.16

RASP Port: 19999

Policy: default policy

Detection Rule ID	Action	Description
SQLI	Detect	Detect and defend against SQ...
SuspiciousBehavior	Detect	Detect suspicious behaviors.
SuspiciousException	Detect	Detect suspicious exceptions.
WebShellUpload	Detect	Detect and defend against att...

Table 6-4 Parameters for adding a protected server

Parameter	Description	Example Value
OS	Server OS type. It can be Linux or Windows.	**Linux**
RASP Port	RASP listening port.	**19999**

Parameter	Description	Example Value
Policy	Application protection policy. HSS provides the **default policy**, which contains 16 detection rules. If the default policy is not applicable to your workloads, you can create a custom policy. For details, see **Adding a Protection Policy**.	**default policy**

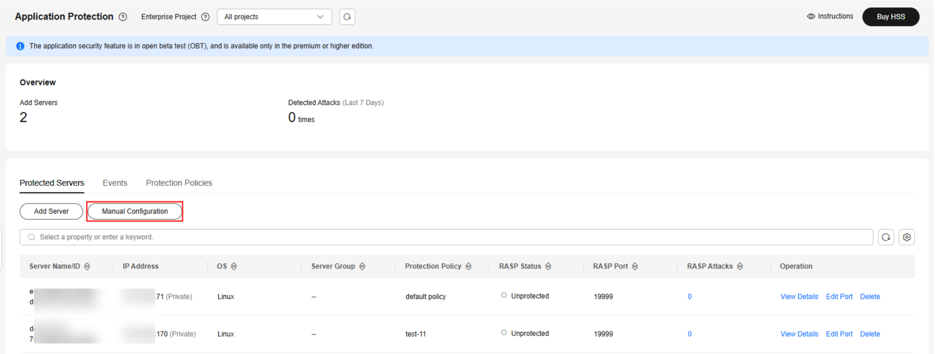
Step 7 On the **Protected Servers** tab page, check whether the **RASP Status** of the server is **Unprotected**.

If the **RASP Status** is **Enabling protection**, the system is installing the RASP plug-in on the server. Wait for several minutes.

Step 8 Manually configure startup parameters for web applications to enable RASP protection.

1. Click **Manual Configuration**. The **Configure Microservice RASP** slide-out panel is displayed.

Figure 6-8 Manual configuration



The application security feature is in open beta test (OBT), and is available only in the premium or higher edition.

Overview

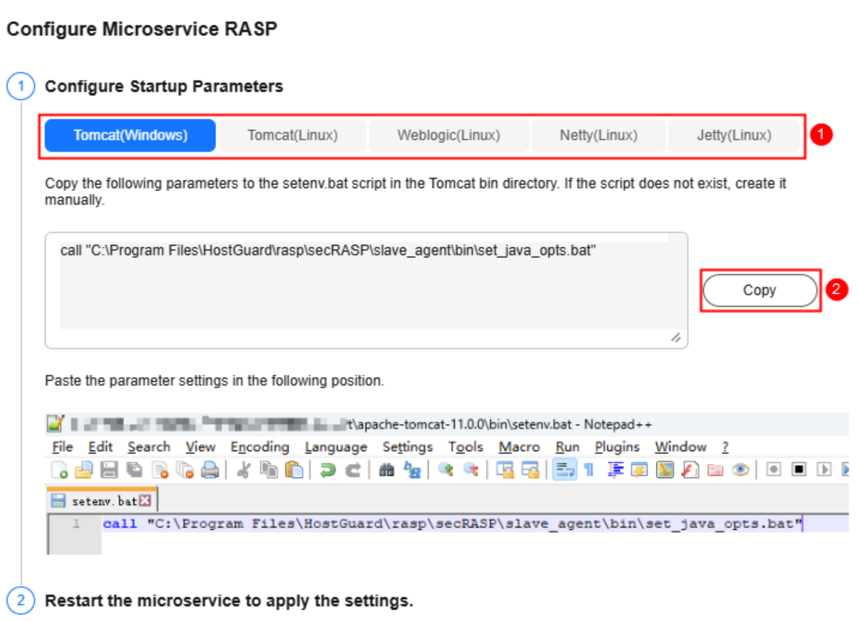
Add Servers
2

Detected Attacks (Last 7 Days)
0 times

Server Name/ID	IP Address	OS	Server Group	Protection Policy	RASP Status	RASP Port	RASP Attacks	Operation
[redacted]	[redacted].71 (Private)	Linux	--	default policy	○ Unprotected	19999	0	View Details Edit Port Delete
[redacted]	[redacted].170 (Private)	Linux	--	test-11	○ Unprotected	19999	0	View Details Edit Port Delete

2. Select a web application. Copy the startup parameters as instructed, and paste the startup parameters to the startup script of the web application.

Figure 6-9 Configuring startup parameters



Configure Microservice RASP

1 Configure Startup Parameters

Copy the following parameters to the setenv.bat script in the Tomcat bin directory. If the script does not exist, create it manually.

```
call "C:\Program Files\HostGuard\rasp\secRASP\slave_agent\bin\set_java_opts.bat"
```

Paste the parameter settings in the following position.

[redacted]t\apache-tomcat-11.0.0\bin\setenv.bat - Notepad++

```
call "C:\Program Files\HostGuard\rasp\secRASP\slave_agent\bin\set_java_opts.bat"
```

2 Restart the microservice to apply the settings.

3. After the startup parameters are set, restart the web application.
4. Wait for 5 to 10 minutes. In the **Operation** column of the server, click **View Details**. The **Application Protection Details** slide-out panel is displayed.
5. Check the RASP protection status of the web application. If the status is **Protected**, it indicates protection has been enabled.

   If a server has multiple web applications, perform the preceding operations for these web applications one by one. If you set startup parameters for only one web application, the protection status of the target server on the **Protected Servers** page will be **Partially protected**.

----End

Related Operations

To change a protected RASP port, click **Edit Port** in the **Operation** column of a server. After the port is changed, the system will restart the RASP plug-in. It will take several minutes.

6.1.3 Viewing Application Protection

Scenario

After application protection is enabled, you can view the protection status and events on the **Application Protection** page. You can analyze the events and harden your applications accordingly.

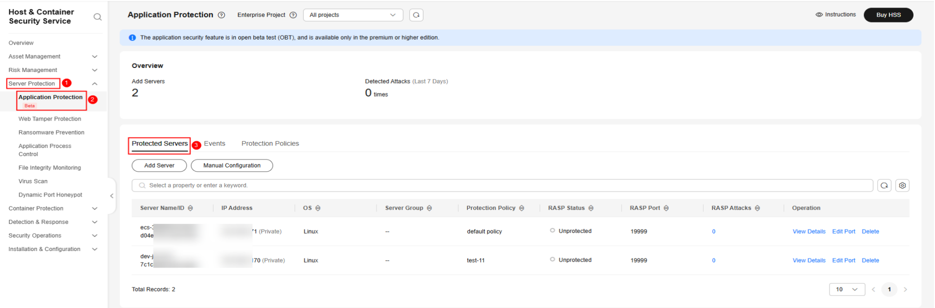
Viewing the Protection Status

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Application Protection**. Click the **Protected Servers** tab.

Figure 6-10 Viewing protection settings



The application security feature is in open beta test (OBT), and is available only in the premium or higher edition.

Overview

Add Servers
2

Detected Attacks (Last 7 Days)
0 times

Server Name/ID	IP Address	OS	Server Group	Protection Policy	RASP Status	RASP Port	RASP Attacks	Operation
ecs-[redacted] d04e	[redacted]1 (Private)	Linux	--	default policy	○ Unprotected	19999	0	View Details Edit Port Delete
dev-j[redacted] 7c1c	[redacted]70 (Private)	Linux	--	test-11	○ Unprotected	19999	0	View Details Edit Port Delete

Total Records: 2

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 View the service protection status. For details, see **Table 6-5**.

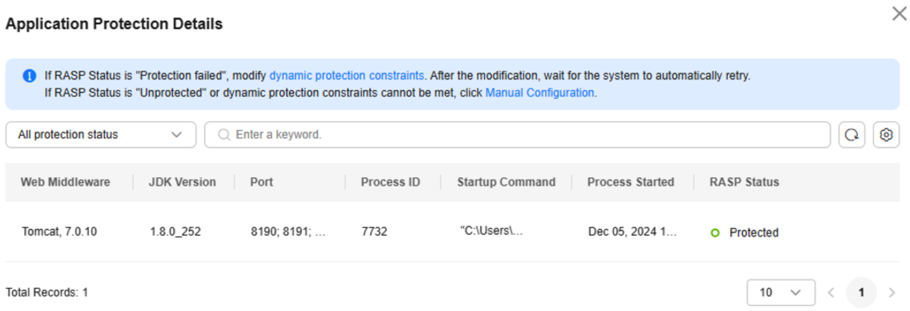
Table 6-5 Parameters for protection settings

Parameter	Description
Server Name/ID	Server name and ID
IP Address	Private IP address and EIP of the server
OS	Server OS
Server Group	Group that the server belongs to
Policy	Detection policies bound to the target server.
RASP Status	Web application protection status. ● **Unprotected**: The server has been added for protection but RASP is not enabled. ● **Protected**: RASP is enabled. ● **Protection failed**: RASP fails to be enabled due to an exception. ● **Partially protected**: RASP fails to be enabled for some middleware.
RASP Port	Port protected by RASP on a server.
RASP Attacks	Application protection events that occurred on the server.

Step 6 In the **Operation** column of the server, click **View Details** to view web protection details.

On the protection details page, you can check the RASP protection status of web applications.

Figure 6-11 Application protection details



Application Protection Details

If RASP Status is "Protection failed", modify dynamic protection constraints. After the modification, wait for the system to automatically retry.
If RASP Status is "Unprotected" or dynamic protection constraints cannot be met, click Manual Configuration.

All protection status | Enter a keyword.

Web Middleware	JDK Version	Port	Process ID	Startup Command	Process Started	RASP Status
Tomcat, 7.0.10	1.8.0_252	8190; 8191; ...	7732	"C:\Users\...	Dec 05, 2024 1...	○ Protected

Total Records: 1

10 < 1 >

----End

Viewing Events

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Server Protection** > **Application Protection** and click the **Events** tab. For more information, see **Table 6-6**.

To view the protection events of a server, click the number in the **Attacks** column of the server on the **Protected Servers** tab page.

Table 6-6 Event parameters

Parameter	Description
Severity	Alarm severity. You can search for servers by alarm severities. ● **Critical** ● **High** ● **Medium** ● **Low**
Server Name	Server that triggers an alarm
Alarm Name	Alarm name
Alarm Time	Time when an alarm is reported
Attack Source IP Address	IP address of the server that triggers the alarm
Attack Source URL	URL of the server that triggers the alarm

Step 3 You can click an alarm name to view the attack information (such as the request information and attack source IP address) and extended information (such as detection rule ID and description), and troubleshoot the problem accordingly.

----End

6.1.4 Managing Application Protection Policies

Scenario

Application protection policies can be added, edited, and deleted in the following scenarios:

- Addition: HSS provides a default policy, which contains all the detection rules for application protection. For details, see **Detection Capabilities**. If you need to customize the policy for a server, you can add a protection policy and customize the detection rules and configurations in the policy.
- Editing: You can edit a custom protection policy.
- Deletion: You can delete a custom protection policy that is not associated with any server.

Adding a Protection Policy

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

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

Step 3 Choose **Server Protection** > **Application Protection** and click **Protection Policies**. For more information, see **Table 6-7**.

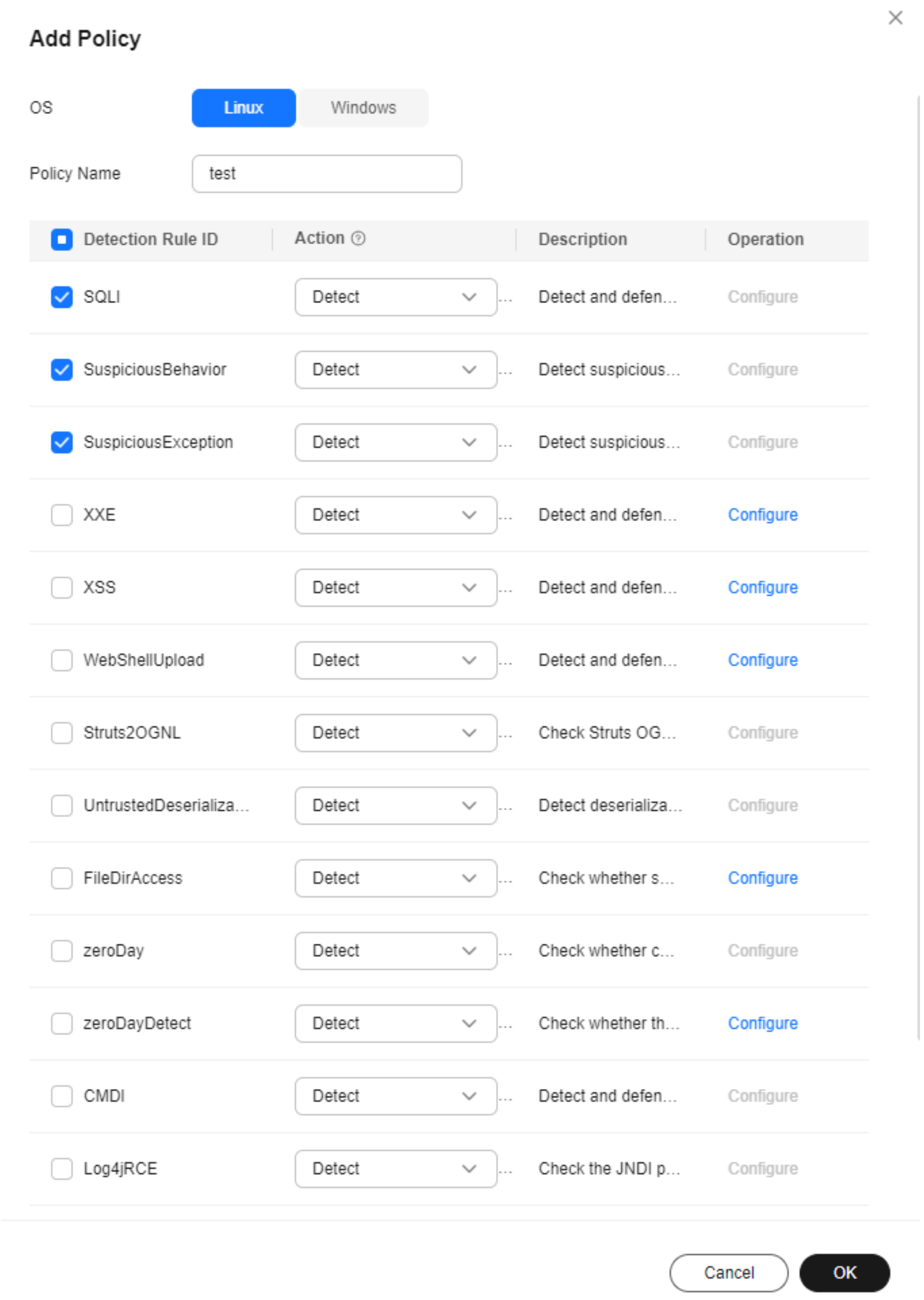
Table 6-7 Protection policy parameters

Parameter	Description
Policy Name	Protection policy name
Detection Rule	Detection rules supported by a policy.
Associated Servers	Number of servers bound to a policy.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click **Add Policy**. In the dialog box that is displayed, configure the parameters by referring to **Table 6-8**.

Figure 6-12 Adding a protection policy



Add Policy

OS: Linux | Windows

Policy Name: test

■ Detection Rule ID	Action	Description	Operation
☑ SQLI	Detect	Detect and defen...	Configure
☑ SuspiciousBehavior	Detect	Detect suspicious...	Configure
☑ SuspiciousException	Detect	Detect suspicious...	Configure
☐ XXE	Detect	Detect and defen...	Configure
☐ XSS	Detect	Detect and defen...	Configure
☐ WebShellUpload	Detect	Detect and defen...	Configure
☐ Struts2OGNL	Detect	Check Struts OG...	Configure
☐ UntrustedDeserializa...	Detect	Detect deserializa...	Configure
☐ FileDirAccess	Detect	Check whether s...	Configure
☐ zeroDay	Detect	Check whether c...	Configure
☐ zeroDayDetect	Detect	Check whether th...	Configure
☐ CMDI	Detect	Detect and defen...	Configure
☐ Log4jRCE	Detect	Check the JNDI p...	Configure

Table 6-8 Application protection policy parameters

Parameter	Description
OS	OS of the servers that the protection policy applies to.
Policy Name	User-defined policy name
Detection Rule ID	Unique ID of a detection rule. To enable a detection rule, select the check box next to the ID.

Parameter	Description
Action	Protection action of a detection rule. ● **Detect**: Detects objects based on the target rule and reports alarms for detected risk events. ● **Detect and block**: Detects objects based on the target rule, reports alarms for detected risk events, and directly blocks or intercepts detected risk items. **WARNING** Blocking or interception may interrupt services. Exercise caution when enabling this function.
Description	Description about the detected object and behavior of the target protection policy.

Step 6 Click **Configure** in the **Operation** column of a detection rule to modify the rule content. **Table 6-9** describes the supported detection rules.

Table 6-9 Detection rules that can be configured only

Rule	Description	Example
XXE	User-defined XXE blacklist protocol	.xml;.dtd;
XSS	User-defined XSS shielding rules	xml;doctype;xmlns;import;entity
WebShellUpload	User-defined suffix of files in the blacklist.	.jspx;.jsp;.jar;.phtml;.asp;.php;.ascx;.ashx;.cer
FileDirAccess	User-defined path of files in the blacklist.	/etc/passwd;/etc/shadow;/etc/gshadow;

Step 7 Confirm the configured policy and selected detection rules, and click **OK**. You can check whether the rule is added on the **Protection Policy** tab page.

----End

Editing a Protection Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Server Protection** > **Application Protection** and click **Protection Policies**. For more information, see **Table 6-10**.

Table 6-10 Protection policy parameters

Parameter	Description
Policy Name	Protection policy name

Parameter	Description
Detection Rule	Detection rules supported by a policy.
Associated Servers	Number of servers bound to a policy.

Step 3 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 4 Click **Edit** in the **Operation** column of a policy to configure the policy name, supported detection rules, and rule content.

Table 6-11 Application protection policy parameters

Parameter	Description
Policy Name	User-defined policy name
Detection Rule ID	Unique ID of a detection rule. To enable a detection rule, select the check box next to the ID.
Action	Protection action of a detection rule. ● **Detect**: Detects objects based on the target rule and reports alarms for detected risk events. ● **Detect and block**: Detects objects based on the target rule, reports alarms for detected risk events, and directly blocks or intercepts detected risk items. **NOTICE** Blocking or interception may interrupt services. Exercise caution when enabling this function
Description	Description about the detected object and behavior of the target protection policy.

Step 5 Confirm the configured rule and selected detection items and click **OK**. You can check whether the target policy is modified on the **Protection Policy** tab page.

----End

Deleting a Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Server Protection** > **Application Protection** and click **Protection Policies**. For more information, see **Table 6-12**.

Table 6-12 Protection policy parameters

Parameter	Description
Policy Name	Protection policy name

Parameter	Description
Detection Rule	Detection rules supported by a policy.
Associated Servers	Number of servers bound to a policy.

Step 3 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 4 Click **Delete** in the **Operation** column of the target policy. In the dialog box that is displayed, confirm the policy information and click **OK**.

NOTICE

Only the policies that are not associated with any server can be deleted.

----End

6.1.5 Disabling Application Protection

Scenario

You can disable application protection if it is no longer needed.

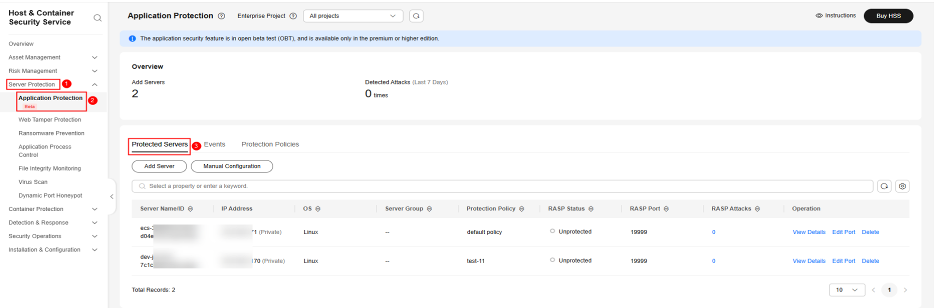
Disabling Application Protection

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Application Protection**. Click the **Protected Servers** tab.

Figure 6-13 Viewing protection settings



The application security feature is in open beta test (OBT), and is available only in the premium or higher edition.

Overview

Add Servers
2

Detected Attacks (Last 7 Days)
0 times

Server Name/ID	IP Address	OS	Server Group	Protection Policy	RASP Status	RASP Port	RASP Attacks	Operation
ecs-[redacted] d04e[redacted]	[redacted]1 (Private)	Linux	--	default policy	○ Unprotected	19999	0	View Details Edit Port Delete
dev-[redacted] 7c1c[redacted]	[redacted]70 (Private)	Linux	--	test-11	○ Unprotected	19999	0	View Details Edit Port Delete

Total Records: 2

10 < 1 >

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click **Delete** in the **Operation** column of a server.

Step 6 In the **Delete** dialog box, confirm the information about the server where application protection is to be disabled, enter **DELETE**, and click **OK**.

----End

6.2 WTP

6.2.1 WTP Overview

What Is Web Tamper Protection?

If your websites and applications have vulnerabilities, attackers can exploit them to obtain permissions, tamper with web pages or put hidden links on websites to spread malicious information. This may lead to information leak, website interruption, economic loss, bad brand image, and even lawsuits.

Web Tamper Protection (WTP) uses technologies to prevent tampering and protect website integrity.

The HSS WTP can detect and prevent tampering of files in specified directories, including web pages, documents, and images, and quickly restore them using valid backup files.

Constraints

Web tamper protection is available only in the HSS WTP edition. For details about how to purchase HSS and enable the WTP edition, see **Purchasing an HSS Quota** and **Enabling Web Tamper Protection**.

How WTP Prevents Web Page Tampering

WTP supports static and dynamic web page protection. **How WTP works** shows the protection mechanism.

Table 6-13 How WTP works

Protection Type	Mechanism
Static web page protection	1. Local directory lock WTP locks files in a web file directory in a drive to prevent attackers from modifying them. Website administrators can update the website content by using privileged processes. 2. Active backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local host to restore the file. 3. Remote backup and restoration After a remote backup server is configured, if a file in a protected directory is changed, HSS will back up the updated file. If the file and backup directory on the local server become invalid, you can log in to the remote backup server, obtain backup files, and manually restore the tampered websites. You can view backup paths on the **Manage Remote Backup Server** page. For details, see **Modifying a Remote Backup Server**.
Dynamic web page protection	The Huawei-proprietary RASP can detect application program behaviors, prevent attackers from tampering with web pages through application programs, and provide self-protection in Tomcat application runtime.

Scenarios

WTP can protect sensitive website data in diverse scenarios, for example:

- Government institutions release important policy information, laws, and regulations on websites.
- Financial websites provide information and services of banks, securities companies, and other financial institutions.
- E-commerce platforms release product information, prices, and promotional activities.
- News websites release news.
- Companies and institutions put their overview, product introduction, and service information on websites.

WTP protects websites from being tampered with, ensuring information correctness and integrity.

Process of Using WTP

Figure 6-14 Usage process

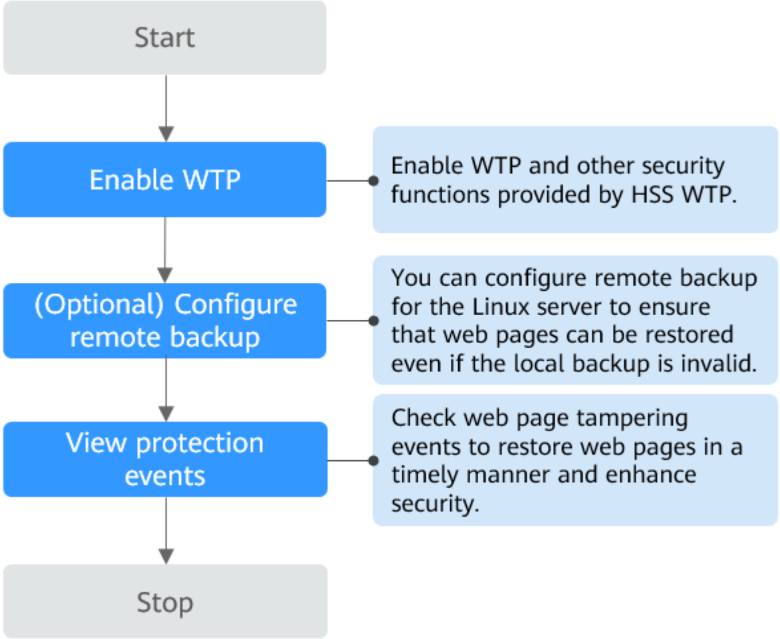

Start
Enable WTP
Enable WTP and other security functions provided by HSS WTP.
(Optional) Configure remote backup
You can configure remote backup for the Linux server to ensure that web pages can be restored even if the local backup is invalid.
View protection events
Check web page tampering events to restore web pages in a timely manner and enhance security.
Stop

Table 6-14 Process of using WTP

Operation	Description
Enabling the WTP Edition	Enable the WTP edition to enjoy the web tamper protection provided by HSS. For details, see **Features**. When enabling WTP, select servers and configure protection policies (protected directories, scheduled protection, privileged processes, and dynamic WTP).
(Optional) **Configuring Remote Backup**	By default, for Linux servers, HSS backs up the files in the protected directories to the local backup paths you specified. For stronger security, you can configure remote backup, so that your data can still be restored even if the local backup is damaged.
Viewing WTP Events	Tamper events that occur during web tamper protection are recorded and displayed in the event list.

Related Operations

After WTP is enabled, files and folders in the protected directory will be set to read-only and cannot be modified. To update a web page, you can:

- Configure privileged processes

  You can configure privileged processes to modify files in protected directories. For details, see **Modifying WTP Configuration**.

- Configure scheduled protection

  You can configure an unprotected period. In this period, static web page protection is automatically disabled and you can update web pages. For details, see **Modifying WTP Configuration**.

- Manually enable or disable protection on directories

  You can disable protection for protected directories, update web pages, and enable protection again. For details, see **Manually Enabling or Disabling Directory Protection**.

FAQ

What Are the Differences Between the Web Tamper Protection Functions of HSS and WAF?

6.2.2 Configuring Remote Backup

Scenarios

To perform remote backup is to back up the data of a server to another server. Currently, it is only supported for Linux servers.

When you enable WTP on a Linux server, specify a local backup path. HSS will back up protected directories to that path. (The user-defined excluded subdirectories and file types will not be configured). Once the files in the protected directories are modified, HSS will automatically restore them.

For higher security, configure remote backup. Even if local server backup is damaged by attackers, you can log in to the remote backup server, go to the backup path, and obtain the remote backup to manually restore tampered web pages. You can view the backup path on the **Manage Remote Backup Servers** page. For details, see **Modifying a Remote Backup Server**.

Constraints

- Only Linux servers support remote backup.
- A remote backup server must be a Huawei Cloud Linux server. Ensure the server status is **Running**, and the server has an HSS agent in **Online** status.
- The remote backup server must connect to the protected server. To enjoy quick and stable backup, put the two servers in same intranet.

Remote Backup Configuration Process

Perform the following operations:

1. **Adding a Remote Backup Server**
2. **Enabling Remote Backup**

For details about how to modify or disable remote backup, see **Modifying a Remote Backup Server** and **Disabling Remote Backup**.

Adding a Remote Backup Server

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

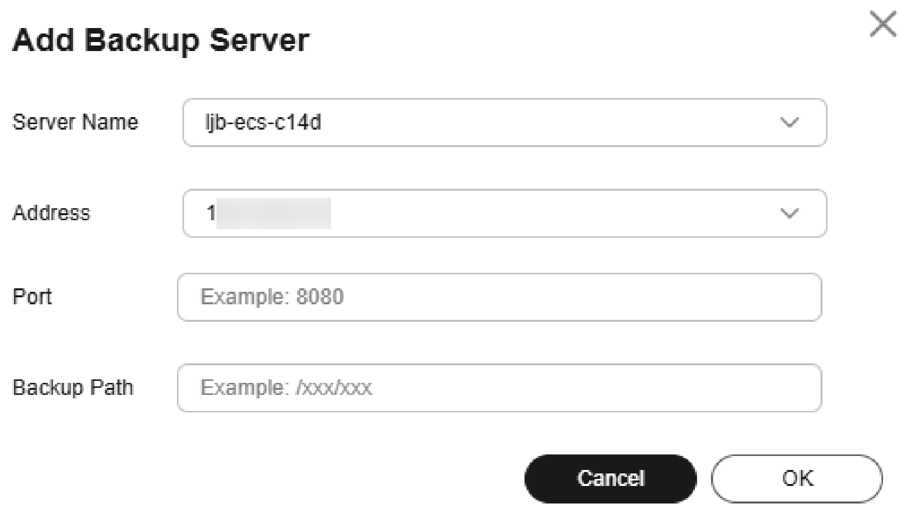
Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Step 4 In the **Operation** column of a server, choose **More** > **Manage Remote Backup Servers**.

Step 5 On the **Manage Remote Backup Servers** page, click **Add Backup Server**.

Step 6 In the dialog box that is displayed, enter backup server information. For more information, see **Table 6-15**.

Figure 6-15 Adding a remote backup server



Add Backup Server

Server Name: ljb-ecs-c14d

Address: 1[redacted]

Port: Example: 8080

Backup Path: Example: /xxx/xxx

Table 6-15 Backup server parameters

Parameter	Description
Server Name	Select a server from the drop-down list.
Address	This parameter will be automatically set after a server is selected.
Port	Enter a port to be used for data backup.

Parameter	Description
Backup Path	Enter a complete backup path. ● A backup path cannot contain semicolons (;), start with a space, or end with a slash (/). Up to 256 characters are allowed. ● Key system directories are a main attack target and cannot be used as backup paths, including but not limited to **/etc/**, **/bin/**, **/usr/bin/**, **/var/spool/**, **/usr/sbin/**, **/sbin/**, **/usr/lib/**, **/lib/**, **/lib64/**, **/usr/lib64/**, and their subdirectories. ● 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**.

Step 7 Click **OK**.

Step 8 On the **Manage Remote Backup Servers** page, check the status of the target server. If the status is **Running**, the remote backup server has been added.

The status of a remote backup server indicates whether the server can be used for backup. For details, see **Table 6-16**.

Table 6-16 Remote backup server status

Status	Description
Not started	The WTP backup policy has not been delivered.
Starting	The WTP backup policy is being delivered.
Running	The WTP backup policy has been delivered. You can start backup.
Startup Failed	The server agent is offline, and the WTP backup policy fails to be delivered.

----End

Enabling Remote Backup

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

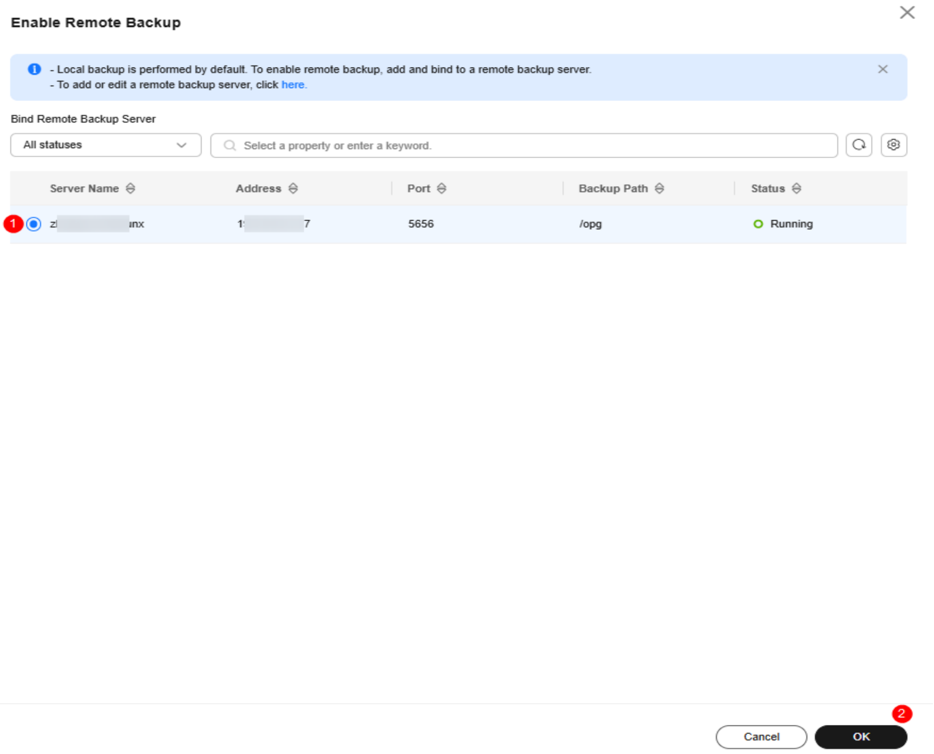
Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Step 4 In the **Operation** column of a server, choose **More** > **Enable Remote Backup**.

Step 5 On the **Enable Remote Backup** page, select a server and click **OK**.

Figure 6-16 Enabling remote backup



Enable Remote Backup

- Local backup is performed by default. To enable remote backup, add and bind to a remote backup server.
- To add or edit a remote backup server, click here.

Bind Remote Backup Server

All statuses

Select a property or enter a keyword.

	Server Name	Address	Port	Backup Path	Status
●	z[redacted]ınx	1[redacted]7	5656	/opg	Running

----End

Modifying a Remote Backup Server

After a remote backup server is added, you can modify its backup path and port.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Step 4 In the **Operation** column of a server, choose **More** > **Manage Remote Backup Servers**.

Step 5 In the **Operation** column of a remote backup server, click **Edit**.

Step 6 In the **Configure Remote Backup Server** dialog box, modify server information.

Step 7 Click **OK**.

Step 8 On the **Manage Remote Backup Servers** page, check the status of the target server. If the status is **Running**, the remote backup server has been modified.

----End

Disabling Remote Backup

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Step 4 Disable remote backup in either of the following ways:

- **Disable remote backup only**
  1. In the **Operation** column of a server, choose **More** > **Disable Remote Backup**.
  2. In the dialog box that is displayed, set **YES** and click **OK**.
- **Disable remote backup and delete the remote backup server**
  1. In the **Operation** column of a server, choose **More** > **Manage Remote Backup Servers**.
  2. In the **Operation** column of a remote backup server, click **Delete**.
  3. In the dialog box that is displayed, click **OK**.

----End

6.2.3 Modifying WTP Configuration

Scenarios

You can modify configuration after WTP is enabled.

You can perform the following operations:

- **Manage protected directories**: Add, modify, or delete protected directories.
- **Configure scheduled protection**: Configure when to enable and disable static WTP. While WTP is disabled, you can update and release web pages. This feature is optional.
- **Enable and disable dynamic WTP**: Enable dynamic WTP to protect Tomcat web pages on Linux servers. It can detect and block the tampering with dynamic data, such as database data, in real time. Currently, dynamic WTP can protect Tomcat applications using JDK 8, JDK 11, and JDK 17.
- **Configure privileged processes**: After static WTP is enabled, the files and folders in protected directories are set to read-only and cannot be modified. You can configure privileged processes to modify them. This feature is compatible with Linux and Windows. For Linux, only the distributions using kernel versions 5.10 or later are supported.

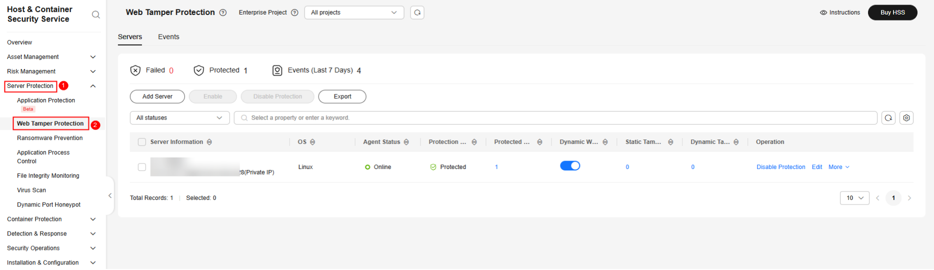
Modifying WTP Settings

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Figure 6-17 Web tamper protection



Server Information	OS	Agent Status	Protection ...	Protected ...	Dynamic W...	Static Tam...	Dynamic Ta...	Operation
[redacted]8(Private IP)	Linux	Online	Protected	1	●	0	0	Disable Protection Edit More

Total Records: 1 | Selected: 0

Step 4 In the **Operation** column of a server, click **Edit**.

Step 5 On the **Edit** page, modify the WTP configuration.

- **Manage protected directories**

  You can add, modify, and delete protected directories.

  – Modify a protected directory

    On the **Edit** page, you can modify excluded file types and protection modes. To modify the directory, excluded subdirectories, excluded file paths, and local backup paths of a protected directory, click **Edit** in its **Operation** column. For details, see **Table 6-17**.

  – Delete a protected directory

    If a directory no longer needs protection, click **Delete** in its **Operation** column.

  – Add a protected directory

    Click **Add Protected Directory**. In the dialog box that is displayed, enter directory information and click **OK**. For details, see **Table 6-17**.

Table 6-17 Protected directory parameters

Parameter	Description	Example Value
Protected Directory	WTP supports static and dynamic web page protection. Static WTP protects specified directories by locking files in the web file directory in the drive to prevent attackers from modifying the files. Therefore, when configuring a protection policy, you need to specify the directories to be protected. After a directory is protected, the files and folders in the directory will become read-only. The requirements for adding a protected directory are as follows: – For Linux, ▪ It cannot start with a space, end with a slash (/), or contain semi-colons (;). Up to 256 characters are allowed. ▪ A server can have up to 50 protected directories. ▪ The folder levels of a protected directory cannot exceed 100. ▪ The total folders in protected directories cannot exceed 900,000. – For Windows, ▪ Up to 256 characters are allowed. The directory name cannot start with a space or end with a backslash (\). It cannot contain the following characters: ;/*?"<>| ▪ A server can have up to 50 protected directories. **Do not add network directories as protected directories.** The reasons are as follows: 1. A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan.	– Linux: **/etc/lesuo** – Windows: **d:\web**

Parameter	Description	Example Value
	2. The access to network directories may occupy all your bandwidth and affect your services.	
Excluded Subdirectory (Optional)	If a protected directory contains subdirectories that do not need to be protected, you can exclude the subdirectories. The requirements for adding a subdirectory are as follows: – A subdirectory name must be a valid relative path of the protected directory. – A subdirectory name cannot start or end with a slash (/) and can contain up to 256 characters. – Up to 10 subdirectories can be added. Use semicolons (;) to separate multiple subdirectories.	– Linux: **lesuo/test** – Windows: **web\test**
Excluded File Path (Optional)	This item is available only for Linux servers. If a protected directory contains files that do not need to be protected, exclude the files. The requirements for adding excluded file paths are as follows: – A file path must be a valid relative path of the protected directory. – A file path cannot start or end with a slash (/), and can contain up to 256 characters. – Up to 50 file paths can be added. Use semicolons (;) to separate multiple file paths.	lesuo/data;lesuo/ma.txt

Parameter	Description	Example Value
Local Backup Path	This item is available only for Linux servers. Set a local backup path for a protected directory. After WTP is enabled, files in the protected directory are automatically backed up to the local backup path. Once the system detects that a file in the protected directory is tampered with, it immediately uses the local backup to restore the tampered file. The requirements for adding local backup paths are as follows: – A local backup path cannot contain semicolons (;), start with a space, or end with a slash (/). Up to 256 characters are allowed. – Key system directories are a main attack target and cannot be used as backup paths, including but not limited to **/etc/**, **/bin/**, **/var/spool/**, **/usr/bin/**, **/usr/sbin/**, **/sbin/**, **/usr/lib/**, **/lib/**, **/lib64/**, **/usr/lib64/**, and their subdirectories. Local backup rule description: – 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.	/etc/backup
Excluded File Type	If a protected directory contains files of certain types that do not need to be protected, exclude these file types, for example, logs. You can exclude any type of files. To record the running status of servers in real time, exclude the log files in the protected directory. You can set high permission requirements for log read and write, so that attackers cannot view or tamper with log files.	log

Parameter	Description	Example Value
Type	Action taken when file tampering is detected. – **Alarm**: Only alarms are reported. – **Block**: An alarm is reported, and the file is restored to the status before being tampered with.	Block

- **Configure scheduled protection**

  Configure when to enable and disable static WTP. While WTP is disabled, you can update and release web pages. Exercise caution when you configure this parameter, because files will not be protected in those periods.

  – : Scheduled protection is enabled.

  – : Scheduled protection is enabled. You need to configure **Unprotected Time Range** and **Unprotected Days of a Week**. For details, see **Table 6-18**.

Table 6-18 Scheduled protection parameters

Parameter	Description	Example Value
Unprotected Time Range	A time range when WTP is disabled within a day, for example, 10:05 to 15:35. Requirements: ■ A time range must be at least 5 minutes. ■ Time ranges (except for those starting at 00:00 or ending at 23:59) cannot overlap and must have at least a 5-minute interval. ■ All time ranges are subject to the system time of the server.	10:05-15:35

Parameter	Description	Example Value
Unprotected Days of a Week	Static WTP is automatically disabled on specified days of a week, for example, Wednesday and Thursday.	Wednesday

- **Enable and disable dynamic WTP**

  Enable dynamic WTP to protect Tomcat web pages on Linux servers. It can detect and block the tampering with dynamic data, such as database data, in real time.

  – ○: Dynamic WTP is disabled.

  – ●: Dynamic WTP is enabled. You need to configure the Tomcat bin directory, for example, **/usr/workspace/apache-tomcat-8.5.15/bin**. The **setenv.sh** script will be put in the bin directory to configure the startup parameters of the anti-tamper program.

- **Configure privileged processes**

  A privileged process is a process authorized to modify a protected directory.

  – ○: Privileged processes are disabled.

  – ●: Privileged processes are enabled. You need to configure **Process File Path** and **Trust Subprocess**. For details, see **Table 6-19**.

Table 6-19 Privileged process parameters

Parameter	Description	Example Value
Process File Path	Set one or multiple complete file paths of privileged processes. Example: ▪ Linux: **/Path/Software.type** ▪ Windows: **C:\Path\Software.type** Put each privileged process file path on a separate line. Up to 10 privileged processes are allowed.	/Path/Software.type

Parameter	Description	Example Value
Trust Subprocess	If **Trust Subprocess** is enabled, HSS will trust all the subprocesses up to five levels deep in the subdirectories of specified directories, and allow the subprocesses to modify protected directories. Subprocesses can modify protected directories.	Enabled

Step 6 Confirm the settings. On the **Edit** page, click **OK**.

After dynamic WTP is enabled for a server, restart Tomcat to apply this setting.

Step 7 Verify the change.

- Protected Directory

  In the **Protected Directories** column of a server, click the number view details.

  If the information about the protected directory is correct and the **Protection Status** is **Protected**, the directory is successfully added or modified.

  If the deleted protected directory is not displayed in the list, its deletion is successful.

- Scheduled protection

  Modify the web page in the specified unprotected period. If it can be modified, the scheduled protection is configured successfully.

- Dynamic WTP

  If the dynamic WTP status is ●, it is enabled.

- Privileged process

  If the web page can be modified through a privileged process, the process is successfully configured.

----End

6.2.4 Manually Enabling or Disabling Directory Protection

Scenarios

Once a directory is protected, all the files and folders in the directory will be set to read-only and cannot be modified. If anyone attempts to modify a file or website, the system will automatically restore it to the status before the modification.

If you need to update a web page immediately, and the scheduled protection and privileged processes cannot help, you can manually disable protection on the directory, update the web page, and enable protection again. For details about scheduled protection and privileged processes, see **Enabling Web Tamper Protection**.

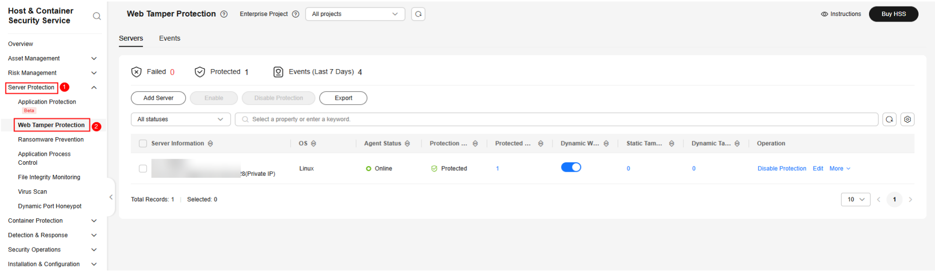
Manually Suspending Directory Protection

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Figure 6-18 Web tamper protection

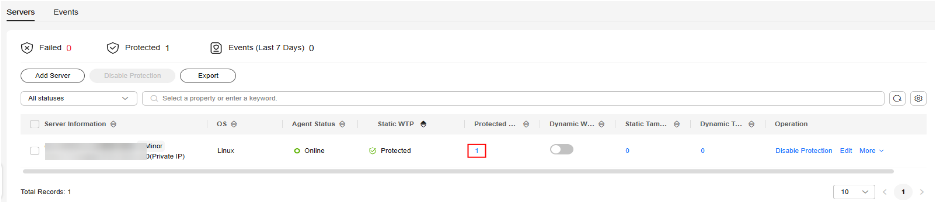


Server Information	OS	Agent Status	Protection ...	Protected ...	Dynamic W...	Static Tam...	Dynamic Ta...	Operation
[redacted]8(Private IP)	Linux	Online	Protected	1	●	0	0	Disable Protection Edit More

Total Records: 1 | Selected: 0

Step 4 In the **Protected Directories** column of a server, click the number to go to the details page.

Figure 6-19 Number of protected directories



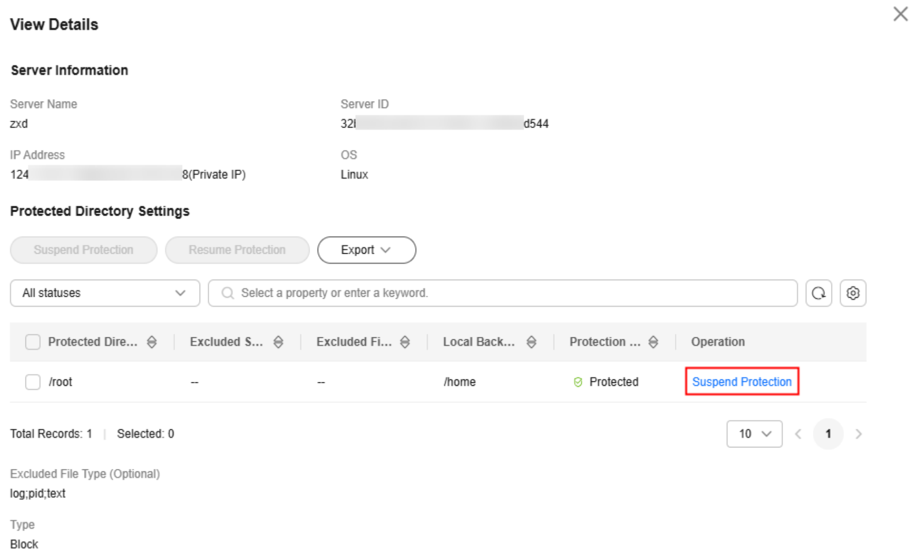
Server Information	OS	Agent Status	Static WTP	Protected ...	Dynamic W...	Static Tam...	Dynamic T...	Operation
[redacted]Minor 0(Private IP)	Linux	Online	Protected	1	○	0	0	Disable Protection Edit More

Total Records: 1

Step 5 In the **Operation** column of a protected directory, click **Suspend Protection**.

To suspend protection for multiple directories, select all the directories and click **Suspend Protection** above the list.

Figure 6-20 Suspending protection



View Details

Server Information

Server Name
zxd

Server ID
32l[redacted]d544

IP Address
124[redacted]8(Private IP)

OS
Linux

Protected Directory Settings

Protected Dire...	Excluded S...	Excluded Fi...	Local Back...	Protection ...	Operation
/root	--	--	/home	Protected	Suspend Protection

Total Records: 1 | Selected: 0

Excluded File Type (Optional)
log;pid;text

Type
Block

Step 6 In the dialog box that is displayed, click **OK**.

If the protection status of the directory is **Unprotected**, the protection has been suspended.

----End

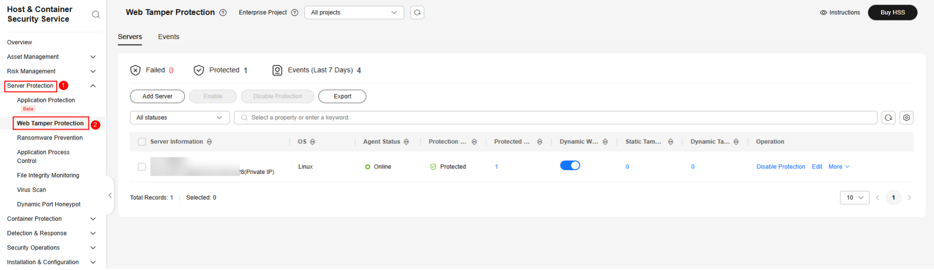
Manually Resuming Directory Protection

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Figure 6-21 Web tamper protection

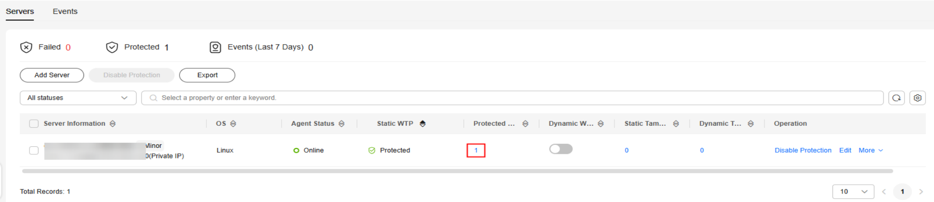


Server Information	OS	Agent Status	Protection ...	Protected ...	Dynamic W...	Static Tam...	Dynamic Ta...	Operation
[redacted] 8(Private IP)	Linux	Online	Protected	1		0	0	Disable Protection Edit More

Total Records: 1 Selected: 0

Step 4 In the **Protected Directories** column of a server, click the number to go to the details page.

Figure 6-22 Number of protected directories



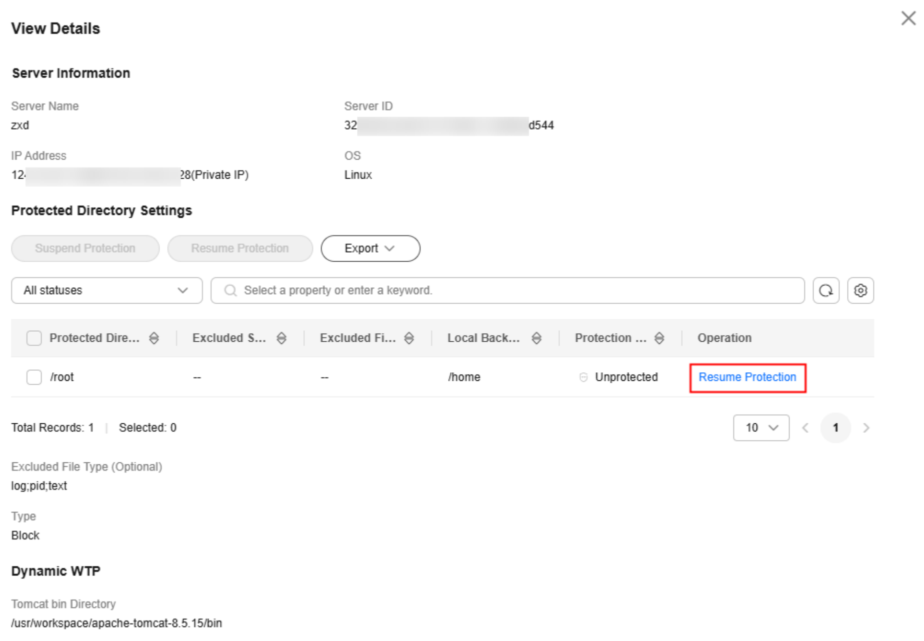
Server Information	OS	Agent Status	Static WTP	Protected ...	Dynamic W...	Static Tam...	Dynamic T...	Operation
[redacted] Minor 0(Private IP)	Linux	Online	Protected	1		0	0	Disable Protection Edit More

Total Records: 1

Step 5 In the **Operation** column of a protected directory, click **Resume Protection**.

To resume protection for multiple directories, select all the directories and click **Resume Protection** above the list.

Figure 6-23 Resuming protection



View Details

Server Information

Server Name
zxd

Server ID
32[redacted]d544

IP Address
12[redacted]28(Private IP)

OS
Linux

Protected Directory Settings

□ Protected Dire...	Excluded S...	Excluded Fi...	Local Back...	Protection ...	Operation
□ /root	--	--	/home	Unprotected	Resume Protection

Total Records: 1 | Selected: 0

Excluded File Type (Optional)
log;pid;text

Type
Block

Dynamic WTP

Tomcat bin Directory
/usr/workspace/apache-tomcat-8.5.15/bin

Step 6 In the dialog box that is displayed, click **OK**.

If the protection status of the directory is **Protected**, the protection has been resumed.

----End

6.2.5 Deleting WTP Configuration

Scenario

If you have disabled WTP for some servers (by referring to **Disabling HSS**) and do not plan to enable WTP for them again, you can delete the information about these servers, so that it will not affect your future O&M.

You can delete the servers that do not need WTP protection. If the servers are deleted, all the WTP configuration of the servers will be permanently deleted.

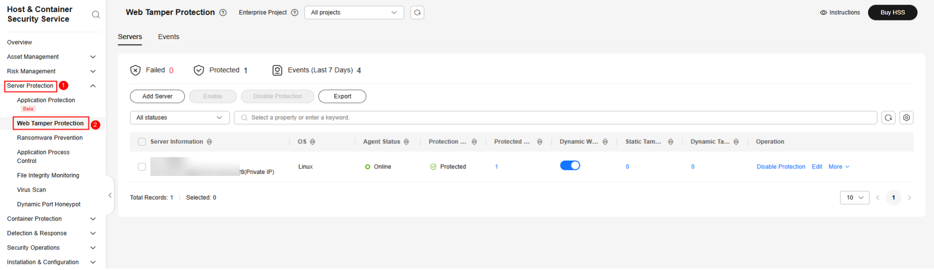
Deleting WTP Configuration

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

Step 2 Click ☰ in the upper left corner of the page, select a region, and choose **Security & Compliance** > **Host Security Service** to go to the HSS management console.

Step 3 In the navigation pane, choose **Server Protection** > **Web Tamper Protection**.

Figure 6-24 Web tamper protection



□	Server Information	OS	Agent Status	Protection ...	Protected ...	Dynamic W...	Static Tam...	Dynamic Ta...	Operation
□	[redacted] :8(Private IP)	Linux	○ Online	✓ Protected	1	●	0	0	Disable Protection Edit More

Step 4 Locate the target server whose **Protection Status** is **Unprotected**.

Step 5 In the **Operation** column of a server, choose **More** > **Delete**. The **Delete WTP Configuration** dialog box is displayed.

Step 6 Confirm the server information to be deleted.

Step 7 Enter **DELETE** in the text box and click **OK**.

If the server is not displayed in the protected server list, it has been deleted.

----End

6.2.6 Viewing WTP Events

Once static WTP is enabled, the HSS service will comprehensively check protected directories you specified. You can check records about detected tampering of host protection files.

Prerequisites

Agent Status of the server is **Online**, and its **WTP Status** is **Enabled**. For more information, see **Viewing Server Protection Status**.

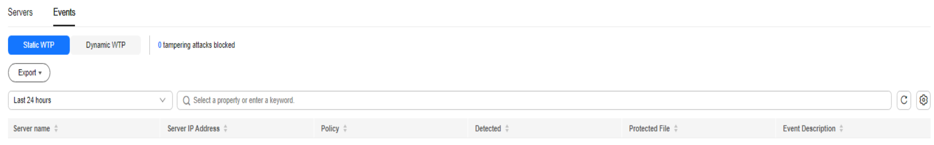
Viewing WTP Events

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

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

Step 3 Choose **Server Protection** > **Web Tamper Protection** and click **Events** to view the tampering records of protected files on servers.

Figure 6-25 Events


Servers
Events
Static WTP
Dynamic WTP
0 tampering attacks blocked
Export
Last 24 hours
Select a property or enter a keyword.

Server name	Server IP Address	Policy	Detected	Protected File	Event Description

----End

6.3 Ransomware Prevention

6.3.1 Ransomware Prevention Overview

What Is Ransomware Prevention?

Ransomware emerged with the Bitcoin economy. It is a Trojan that is disguised as a legitimate email attachment or bundled software and tricks you into opening or installing it. It can also arrive on your servers through website or server intrusion. Once a system is attacked by ransomware, most of its important files will be encrypted. You can obtain file restoration keys only after paying high ransom to the attacker. This not only causes service interruption, data leakage, or data loss, but also lead to economic loss.

HSS provides ransomware prevention to detect and defend against ransomware. It can automatically back up data either at a scheduled time, or immediately if ransomware is detected. This can help you defend against ransomware and reduce loss.

Ransomware Prevention Principles

- **Defending against known ransomware in real time**

  HSS has a virus sample library of billions of samples, covering all the known ransomware families. HSS coordinates local and cloud antivirus. On local servers, it uses the Huawei-proprietary third-generation antivirus engine to detect ransomware attacks. In the cloud antivirus center, it uses behavior analysis, intelligence, AI models, and multi-engine detection to identify and block ransomware.

- **Using honeypots to detect and block unknown ransomware**

  - Linux

    You can deploy static and dynamic honeypot files on servers to make directory traps, capturing possible ransomware encryption behaviors in real time. If the action of a ransomware prevention policy is set to **Report alarm and isolate**, once an abnormal behavior is identified, an alarm will be reported and the file encryption process will be blocked immediately.

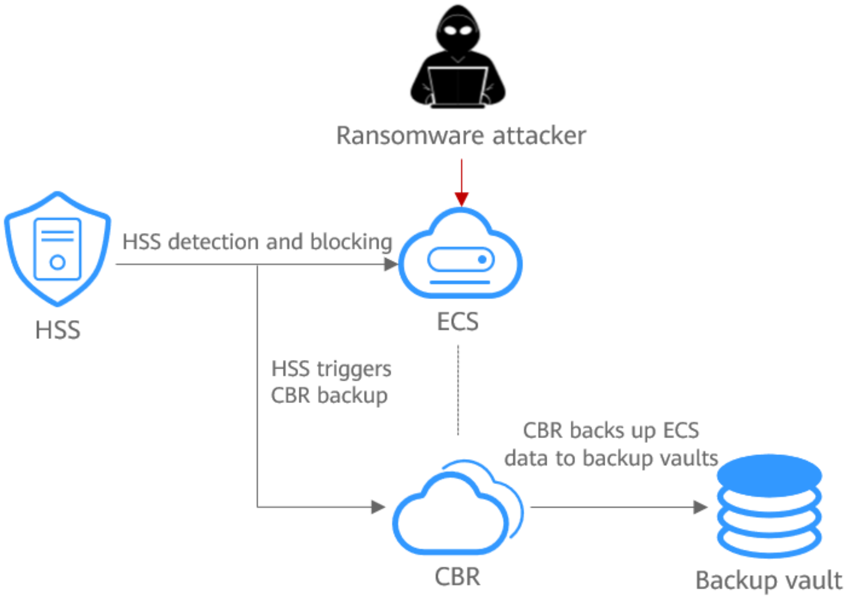
  - Windows

    You can deploy static honeypot files on servers to make directory traps, capturing possible ransomware encryption behaviors in real time. AI ransomware detection algorithms are used to identify the feature segments, fingerprints, and suspicious behaviors of virus-infected files and to block them.

- **Protecting data integrity through backup**

  HSS works with CBR to back up data to defend against ransomware. After this function is enabled, you can configure a policy to periodically back up server data. If a ransomware attack is detected, HSS will immediately trigger backup to ensure server data integrity and reduce service loss.

Figure 6-26 Backup to defend against ransomware



Constraints

- Only the HSS premium, WTP, and container editions support ransomware prevention. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.
- If the agent of version 3.2.10 or later is installed on a Linux server, or the agent of version 4.0.22 or later is installed on a Windows server, and the HSS premium, WTP, or container edition is enabled for the server, HSS will **automatically** enable **ransomware prevention** for the server, but will not automatically enable ransomware backup. You can enable it as needed. If the agent version installed on the server is not in the preceding range, you need to manually enable ransomware prevention and backup.

Process of Using Ransomware Prevention

Figure 6-27 Usage process

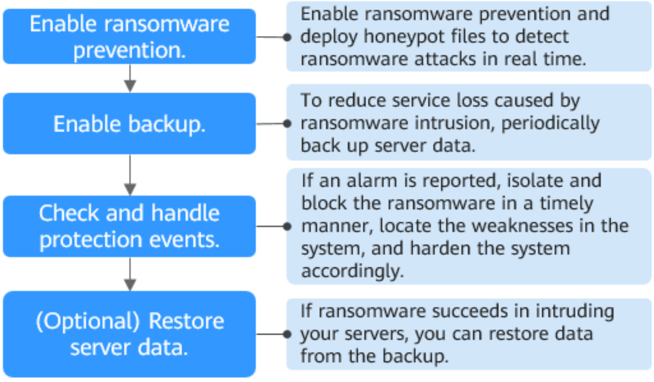

Enable ransomware prevention.
Enable ransomware prevention and deploy honeypot files to detect ransomware attacks in real time.
Enable backup.
To reduce service loss caused by ransomware intrusion, periodically back up server data.
Check and handle protection events.
If an alarm is reported, isolate and block the ransomware in a timely manner, locate the weaknesses in the system, and harden the system accordingly.
(Optional) Restore server data.
If ransomware succeeds in intruding your servers, you can restore data from the backup.

Table 6-20 Usage process

Operation	Description
Enabling Ransomware Prevention	Enable ransomware prevention for a server, deploy static and dynamic honeypots, and detect ransomware attacks in real time. **CAUTION** If you find suspicious files on a server after enabling ransomware prevention, **submit a service ticket** to contact technical support and check whether the files are the honeypots deployed by HSS. Honeypot files are used to detect ransomware attacks. They do not affect your services, do not contain any malicious content, and cannot be manually deleted. ● If the agent of version 3.2.10 or later is installed on a Linux server, or the agent of version 4.0.22 or later is installed on a Windows server, and the HSS premium, WTP, or container edition is enabled for the server, HSS will **automatically** enable **ransomware prevention** for the server. You can modify the default protection policy settings (including protected directories and actions) as needed. For details, see **Managing Ransomware Protection Policies**. ● If the version of the agent installed on the server is not one of the preceding versions, you need to manually enable ransomware prevention.
Enabling Backup	So far, no tools can defend against all ransomware. Servers need to be periodically backed up, so that data can be restored using the backup in a timely manner to reduce loss if a ransomware event occurs.
Viewing and Handling Ransomware Prevention Events	Once a ransomware attack is detected during ransomware protection, analyze and isolate the ransomware in a timely manner, and fix the security weaknesses of the system.
(Optional) Restoring Server Data	If ransomware intrusion succeeds and your service data is lost, you can use the backup to restore data and reduce loss.

6.3.2 Enabling Ransomware Prevention

Scenarios

Ransomware prevention can detect and defend against known and unknown ransomware in real time. You are advised to enable it for every server.

If the agent version of a server is one of the following versions, and you enable the HSS premium, WTP, or container security edition for it, HSS will automatically **enable ransomware prevention for the server**, deploy honeypot files on the server, and automatically isolate suspicious processes. (There is a low probability that some normal processes are incorrectly isolated.) After ransomware prevention is automatically enabled, you can modify the default protection policy settings (including protected directories and actions) as needed. For details, see **Managing Ransomware Protection Policies**.

- Linux: The agent version is 3.2.10 or later.
- Windows: The agent version is 4.0.22 or later.

If the agent version of a server is not one of the preceding versions, or ransomware prevention has been disabled, you can perform the operations in this section to enable it.

⚠ CAUTION

If you find suspicious files on a server after enabling ransomware prevention, **submit a service ticket** to contact technical support and check whether the files are the honeypots deployed by HSS. Honeypot files are used to detect ransomware attacks. They do not affect your services, do not contain any malicious content, and cannot be manually deleted.

Step 1: Creating a Protection Policy

Before enabling ransomware prevention, create a ransomware protection policy and configure honeypot protection directories, protected file types, and protection actions.

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

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

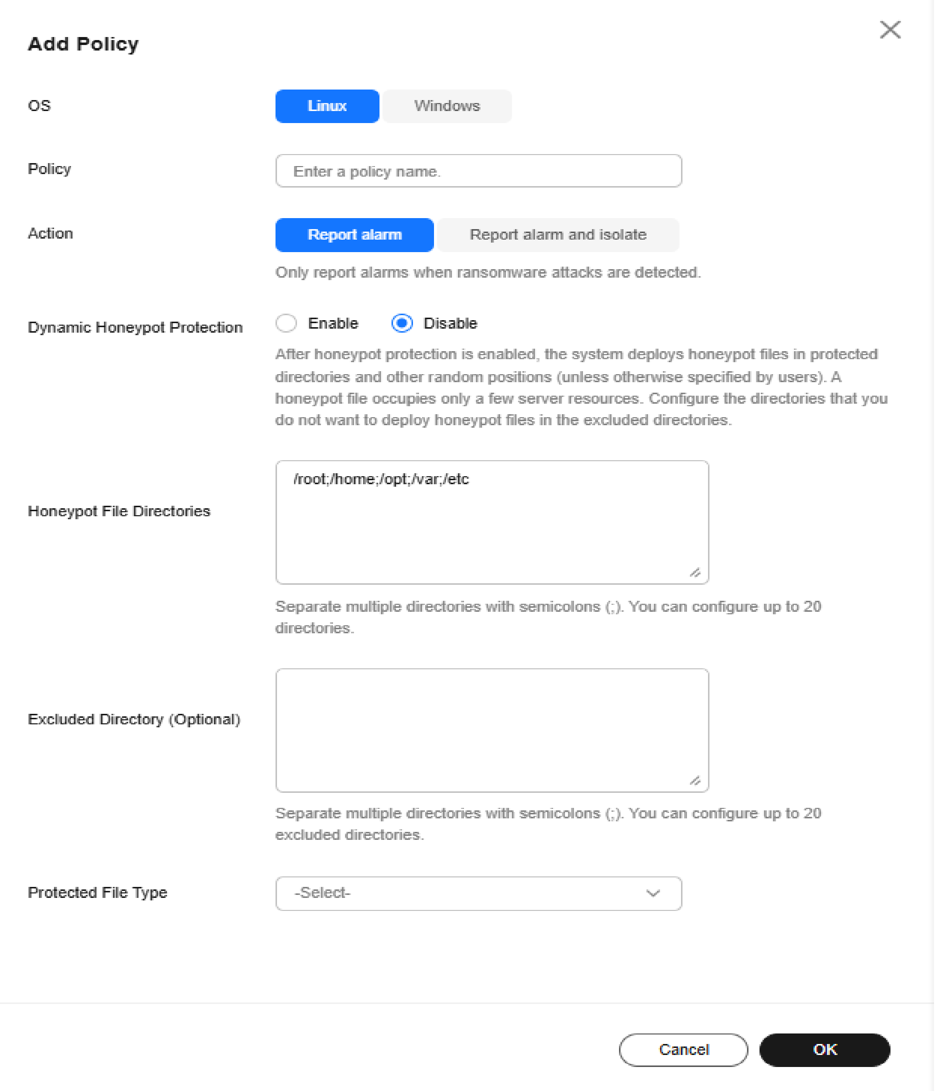
Step 3 Choose **Server Protection** > **Ransomware Prevention**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Policies** tab and click **Add Policy**.

Step 6 Configure policy parameters. For more information, see **Table 6-21**.

Figure 6-28 Protection policy parameters



OS: Linux

Policy: Enter a policy name.

Action: Report alarm

Only report alarms when ransomware attacks are detected.

Dynamic Honeypot Protection: ○ Enable ● Disable

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

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

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

Excluded Directory (Optional):

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

Protected File Type: -Select-

Table 6-21 Protection policy parameters

Parameter	Description	Example Value
OS	Server OS.	Linux
Policy	Policy name.	Anti_Ransomware
Action	How an event is handled. ● **Report alarm and isolate** ● **Report alarm**	**Report alarm and isolate**

Parameter	Description	Example Value
Dynamic Honeypot Protection	After honeypot protection is enabled, the system deploys honeypot files in protected directories and other random locations (unless otherwise specified by users). The honeypot files deployed in random locations are automatically deleted every 12 hours and then randomly deployed again. A honeypot file occupies a few server resources. Therefore, configure the directories that you do not want to deploy the honeypot file in the excluded directories. This parameter is mandatory only for Linux servers.	Enabled
Honeypot File Directories	Directory that needs to be protected by static honeypot (excluding subdirectories). You are advised to configure important service directories or data directories. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	● Linux: /root;/home;/opt;/var;/etc ● Windows: C:\software
Excluded Directory (Optional)	Directory that does not need to be protected by honeypot files. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	● Linux: /bin;/boot;/lib;/lib32;/lib64;/lost+found;/proc;/run;/sbin;/selinux;/srv;/sys;/usr/bin;/usr/local/bin;/usr/local/sbin;/usr/sbin;/var/lib/container;/var/lib/kubelet;/var/lib/ntp/proc ● Windows: C:\software\test

Parameter	Description	Example Value
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. This parameter is mandatory only for Linux servers.	Select all
(Optional) Process Whitelist	Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms. This parameter is mandatory only for Windows servers.	-
AI Ransomware Prevention	It monitors all server files, detects ransomware attack characteristics (including the characteristics of ransomware letters and encryption behaviors) in real time, and determines whether the server is under a ransomware attack. Suspicious events are further checked by the graph engine through comprehensive source tracing analysis to determine whether they are ransomware attacks. For details about graph engine detection, see **Policy Management Overview**. To use the graph engine, you need to enable it and the HIPS policy as well. For details, see **Configuring Policies**. To use AI ransomware prevention, your Windows agent version must be 4.0.28 or later. **This parameter is mandatory only for Windows servers.**	●

Step 7 Click **OK**.

If the added protection policy is displayed in the protection policy list, the policy has been added.

----End

Step 2: Enabling Ransomware Prevention

After a protection policy is created, you can enable ransomware prevention by referring to this section.

Step 1 Log in to the management console.

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

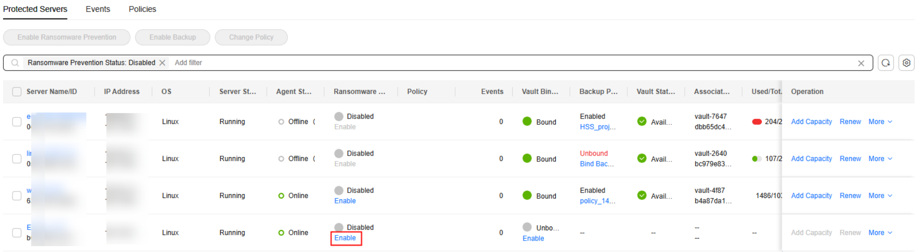
Step 3 Choose **Server Protection** > **Ransomware Prevention**.

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

Step 5 In the **Ransomware Prevention Status** column of a server, click **Enable**.

You can also select multiple servers and click **Enable Ransomware Prevention** above the server list.

Figure 6-29 Enabling



Protected Servers | Events | Policies

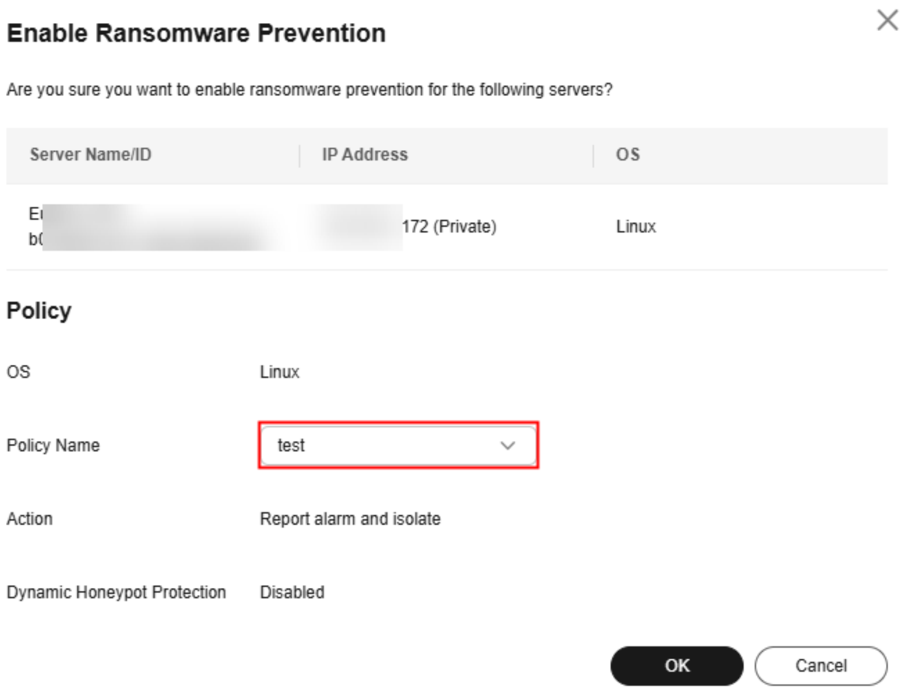
Enable Ransomware Prevention | Enable Backup | Change Policy

Ransomware Prevention Status: Disabled ✕ | Add filter

□	Server Name/ID	IP Address	OS	Server St...	Agent St...	Ransomware ...	Policy	Events	Vault Bin...	Backup P...	Vault Stat...	Associat...	Used/Tot.	Operation
□	[redacted]	[redacted]	Linux	Running	○ Offline (	● Disabled Enable		0	● Bound	Enabled HSS_proj...	✓ Avail...	vault-7647 dbb65dc4...	204/2	Add Capacity Renew More ⌄
□	[redacted]	[redacted]	Linux	Running	○ Offline (	● Disabled Enable		0	● Bound	Unbound Bind Bac...	✓ Avail...	vault-2640 bc979e83...	107/2	Add Capacity Renew More ⌄
□	[redacted]	[redacted]	Linux	Running	○ Online	● Disabled Enable		0	● Bound	Enabled policy_14...	✓ Avail...	vault-4f87 b4a87da1...	1486/10	Add Capacity Renew More ⌄
□	[redacted]	[redacted]	Linux	Running	○ Online	● Disabled Enable		0	● Unbo... Enable	--	--	-- --	--	Add Capacity Renew More ⌄

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

Figure 6-30 Enabling ransomware prevention



Enable Ransomware Prevention

Are you sure you want to enable ransomware prevention for the following servers?

Server Name/ID	IP Address	OS
E[redacted] b[redacted]	[redacted]172 (Private)	Linux

Policy

OS: Linux

Policy Name: test

Action: Report alarm and isolate

Dynamic Honeypot Protection: Disabled

Step 7 Click **OK**.

If the **Ransomware Prevention Status** of the server changes to **Enabled**, ransomware protection is enabled successfully. For details about the ransomware prevention status, see Table 6-22.

Table 6-22 Protection status description

Ransomware prevention status	Description
Protected	Ransomware prevention has been enabled.
Disabled	Ransomware prevention is not enabled.
Enabling	Ransomware prevention is being enabled.
Disabling	Ransomware prevention is being disabled.
Protection failed	Ransomware prevention failed. Rectify the fault by referring to **Ransomware Protection Exception**.
Protection degraded	Honeypot files failed to be deployed in some protected directories. As a result, the protection is degraded. Check whether the **System** group has full control permissions on the protected directories.

----End

FAQ

Ransomware Protection Exception

6.3.3 Enabling Backup

Scenarios

So far, no tools can defend against all ransomware. You can enable backup for servers, so that their data can be restored in a timely manner in the case of a ransomware attack.

Ransomware backup can be performed in two modes: **scheduled backup** and **immediate backup upon ransomware detection**. You can create a custom scheduled backup policy to periodically back up servers. If HSS detects a suspected ransomware attack, it will immediately trigger a backup to ensure service data is stored as much as possible.

This section describes how to enable ransomware backup.

Constraints

Only Huawei Cloud servers support backup to defend against ransomware.

(Optional) Step 1: Purchasing a Backup Vault

You can purchase a backup vault on the HSS console by referring to this section, or on the CBR console by referring to **Creating a Cloud Server Backup**.

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

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

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

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

Step 5 Toggle on ransomware backup. In the dialog box that is displayed, click **Next**.

Step 6 In the displayed dialog box, set the vault parameters.

Table 6-23 Parameters for purchasing backup capacity

Parameter	Description
Billing Mode	Select **Yearly/Monthly** or **On-demand** as required. ● **Yearly/Monthly**: You are billed based on the purchase period specified in the order. ● **On-demand**: You pay for the duration you use the resources. Prices are calculated by hour, and no minimum fee is required.
Region	Region of the backup vault you want to purchase
Capacity	Select the size of the backup vault as required.
Required Duration	Select the required duration if you selected **Yearly/Monthly** for **Billing Mode**.
Price	● **Yearly/Monthly**: You are billed based on the storage capacity and available duration you purchased. ● **On-demand**: You are billed based on the storage capacity you used.

Step 7 Click **OK**.

- If **Yearly/Monthly** is selected:

  a. The order confirmation page is displayed.

  b. Confirm the order and click **Pay**.

- If **On-demand** is selected:

  The capacity is successfully purchased.

⚠ CAUTION

The backup vault will be charged after the ransomware protection is enabled. Ensure that your account balance is sufficient.

----End

Step 2: Enabling Ransomware Backup

Step 1 Log in to the management console.

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

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

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

Step 5 Select a server and click **Enable Backup**.

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

A vault that meets the following conditions can be bound:

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

Step 7 Click **OK**.

If the binding status of the repository on the target server is **Bound**, the ransomware backup is enabled.

----End

6.3.4 Viewing and Handling Ransomware Prevention Events

Scenarios

After ransomware protection is enabled, if a ransomware attack event occurs on the server, the event will be recorded and displayed in the ransomware event list. You can handle the events based on your service requirements.

Constraints

After ransomware protection is enabled, you need to handle ransomware alarms and fix the vulnerabilities in your systems and middleware in a timely manner.

Viewing and Handling Ransomware Prevention Events

Step 1 Log in to the management console.

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

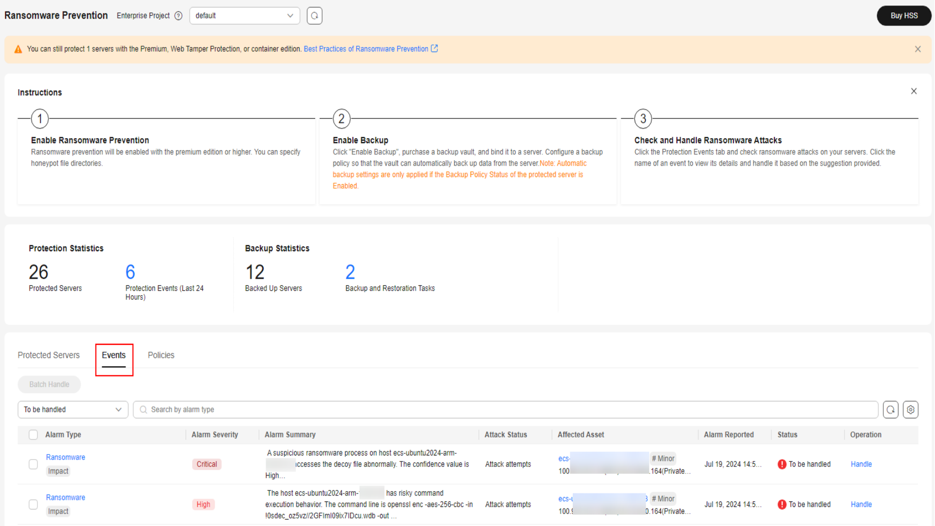
Step 3 Choose **Server Protection** > **Ransomware Prevention**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Events** tab and check events.

To check alarm details, click an alarm name.

Figure 6-31 Viewing protection events



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

Instructions

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

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

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

Protection Statistics: 26 Protected Servers; 6 Protection Events (Last 24 Hours)

Backup Statistics: 12 Backed Up Servers; 2 Backup and Restoration Tasks

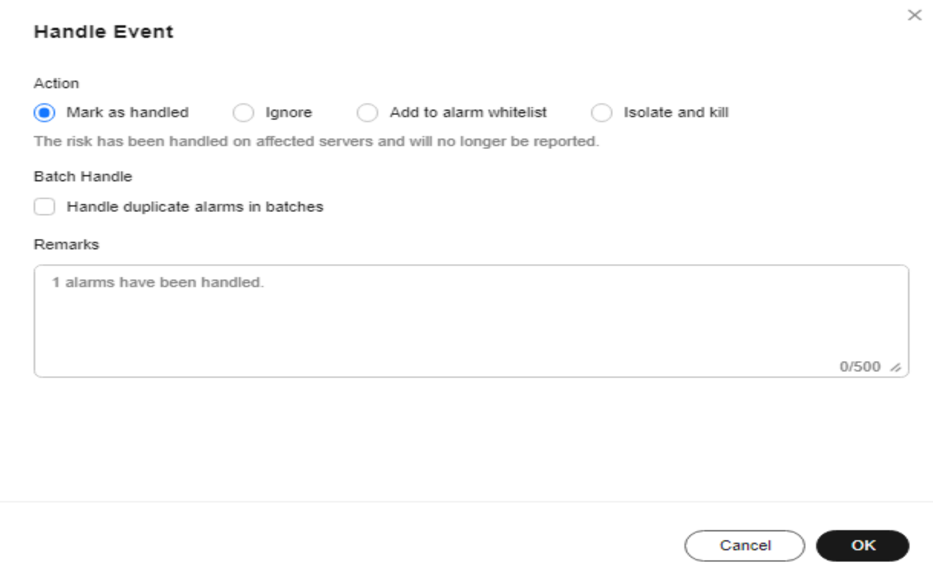
□	Alarm Type	Alarm Severity	Alarm Summary	Attack Status	Affected Asset	Alarm Reported	Status	Operation
□	Ransomware Impact	Critical	A suspicious ransomware process on host ecs-ubuntu2024-arm-[redacted]ccesses the decoy file abnormally. The confidence value is High...	Attack attempts	ecs-[redacted] # Minor 100[redacted].164(Private...	Jul 19, 2024 14:5...	To be handled	Handle
□	Ransomware Impact	High	The host ecs-ubuntu2024-arm-[redacted] has risky command execution behavior. The command line is openssl enc -aes-256-cbc -in !0sdec_oz5vz//2GFImI09ix7IDcu.wdb -out ...	Attack attempts	ecs-[redacted] # Minor 100.[redacted]0.164(Private...	Jul 19, 2024 14:5...	To be handled	Handle

Step 6 After confirming the severity of an event, click **Handle** in the **Operation** column of the target event to handle the event.

You can also select multiple events and click **Batch Handle** above the list to handle events in batches.

Step 7 In the **Handle Event** dialog box, select an action. For details, see **Table 6-24**.

Figure 6-32 Selecting an action



Handle Event

Action

● Mark as handled ○ Ignore ○ Add to alarm whitelist ○ Isolate and kill

The risk has been handled on affected servers and will no longer be reported.

Batch Handle

□ Handle duplicate alarms in batches

Remarks

1 alarms have been handled.

Table 6-24 Alarm handling methods

Parameter	Description
Action	● **Mark as handled** For a manually handled event, you can add remarks to record the details about the event. ● **Ignore** Ignore the current alarm. Any new alarms of the same type will still be reported by HSS. ● **Add to alarm whitelist** Add false alarmed items to the login whitelist. HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms. After adding an alarm to the alarm whitelist, you can customize a whitelist rule. The custom rule types vary depending on the alarm types, including the file path, process path, process command line, remote IP address, and user name. By default, HSS automatically fills in the rule based on the alarm summary. You can modify the rule as required. If a detected alarm event hit the rule you specified, HSS does not generate an alarm. ● **Isolate and kill** If a program is isolated and killed, its executable file status will change to read-only, and the program will be terminated immediately. To avoid impact on services, exercise caution when performing this operation. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check the files. For details, see **Managing Isolated Files**.
Batch Handle	If this option is selected, the same alarms triggered at different time are handled in batches. If no duplicate alarm is displayed after you select it, it indicates no duplicate alarms have been generated.
Remarks	You can add remarks for convenient backtracking.

Step 8 Click **OK**.

----End

6.3.5 Managing Ransomware Protection Policies

Scenarios

After ransomware prevention is enabled, you can manage its policies as needed. Supported operations include:

- **Changing a Policy**: If the current protection policy bound to a server cannot meet your requirements, you can bind another policy to the server.

- **Modifying a Policy**: If you need to modify specific settings (such as the honeypot protection directories or excluded directories), you can modify them in an existing protection policy. When HSS automatically enables ransomware prevention, a protection policy is configured by default. (The default policy for Linux is **tenant_linux_anti_default_policy**, and that for Windows is **tenant_Windows_anti_default_policy**.) You can modify them as needed.
- **Deleting a Policy**: If a protection policy is discarded and not associated with any servers, you can delete the policy.

Changing a Policy

Step 1 Log in to the management console.

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

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

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

Step 5 Select a server and click **Change Policy**.

You can also choose **More** > **Change Policy** in the **Operation** column of a server.

Step 6 In the **Change Policy** dialog box, select a protection policy.

Step 7 Click **OK**.

----End

Modifying a Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Server Protection** > **Ransomware Prevention**. Click the **Policies** tab.

Step 3 Click **Edit** in the **Operation** column of a policy. Edit the policy configurations and associated servers. For more information, see **Table 6-25**.

The following uses a Linux server as an example. On the **Protected Servers** tab, you can also click the name of the policy associated with the server to edit the policy.

Table 6-25 Protection policy parameters

Parameter	Description	Example Value
Policy	Policy name.	Anti_Ransomware
Action	How an event is handled. ● **Report alarm and isolate** ● **Report alarm**	Report alarm and isolate

Parameter	Description	Example Value
Dynamic Honeypot Protection	After honeypot protection is enabled, the system deploys honeypot files in protected directories and other random locations (unless otherwise specified by users). A honeypot file occupies only a few server resources. You can configure excluded directories, so that honeypot files will not be deployed in them. This parameter is mandatory only for Linux servers.	Enabled
Honeypot File Directories	Directory that needs to be protected by static honeypots (excluding subdirectories). You are advised to configure important service directories or data directories. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	● Linux: /root;/home;/opt;/var;/etc ● Windows: C:\software
Excluded Directory (Optional)	Directory that does not need to be protected by honeypot files. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	● Linux: /bin;/boot;/lib;/lib32;/lib64;/lost+found;/proc;/run;/sbin;/selinux;/srv;/sys;/usr/bin;/usr/local/bin;/usr/local/sbin;/usr/sbin;/var/lib/container;/var/lib/kubelet;/var/lib/ntp/proc ● Windows: C:\software\test
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. **This parameter is mandatory only for Linux servers.**	Select all

Parameter	Description	Example Value
(Optional) Process Whitelist	Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms. **This parameter is mandatory only for Windows servers.**	-
Associate Servers	Information about the server associated with the policy. If you want to disassociate the server (disable ransomware protection), you can delete the policy.	-
AI Ransomware Prevention	It monitors all server files, detects ransomware attack characteristics (including the characteristics of ransomware letters and encryption behaviors) in real time, and determines whether the server is under a ransomware attack. Suspicious events are further checked by the graph engine through comprehensive source tracing analysis to determine whether they are ransomware attacks. For more information about graph engine detection, see **Policy Management Overview**. To use the graph engine, you need to enable it and the HIPS policy as well. For details, see **Configuring Policies**. To use AI ransomware prevention, your Windows agent version must be 4.0.28 or later. This parameter is mandatory only for Windows servers.	●

Step 4 Confirm the policy information and click **OK**.

----End

Deleting a Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Server Protection** > **Ransomware Prevention**. Click the **Policies** tab.

Step 3 Click **Delete** in the **Operation** column of the target policy.

NOTE

After a policy is deleted, the associated servers are no longer protected. Before deleting a policy, you are advised to bind its associated servers to other policies.

Step 4 Confirm the policy information and click **OK**.

----End

6.3.6 Restoring Server Data

Scenarios

If ransomware backup is enabled for a server, and the server is intruded by ransomware, you can use the backup to restore the server data and minimize losses. Before using the backup for server restoration, check whether the backup is normal. If it is, use it to restore service-critical systems first.

Prerequisites

The backup function has been enabled. For details, see **Enabling Backup**.

Restoring Server Data

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Server Protection** > **Ransomware Prevention**. Click the **Protected Servers** tab. In the **Operation** column of the target server, click **More** > **Restore Data**.

Step 3 In the displayed dialog box, view the information about the target server. Search for the backup data source to be restored by backup status and backup name. For details about the parameters, see **Table 6-26**.

Table 6-26 Backup data source parameters

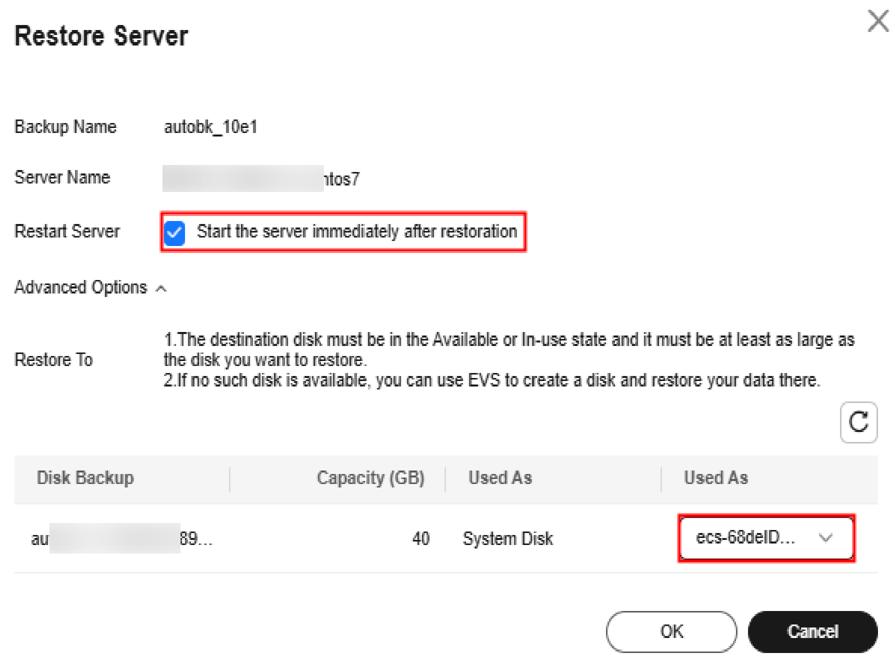
Parameter	Description	Example Value
Backup Name	Name of a backup file.	-
Status	Backup status. It can be: ● **Available**: The backup data source is normal and can be used for restoration. ● **Creating**: The backup is being created. ● **Deleting**: The backup is being deleted. ● **Restoring**: The backup is being used for restoration. ● **Error**: Backup error.	Available

Parameter	Description	Example Value
Purpose	Backup purpose. It can be: ● **Periodic execution**: Data is automatically backed up based on the backup period configured in the backup policy. ● **Ransomware protection**: Data is backed up immediately when a server is attacked by ransomware.	Periodic execution
Execution Time	Time when the data source was backed up.	-

Step 4 In the **Operation** column of a backup, click **Restore Data**.

Step 5 In the displayed dialog box, confirm the server information and click **OK**.

Figure 6-33 Restoring a server



Restore Server

Backup Name autobk_10e1

Server Name [redacted]ntos7

Restart Server ☑ Start the server immediately after restoration

Advanced Options ^

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

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

Step 6 In the **Backup Statistics** column, click the value of **Backup and Restoration Task** to view the backup and restoration progress.

----End

Related Operations

Deleting a backup

You can delete the backup data of a server if it is no longer required. A deleted backup cannot be restored. Exercise caution when performing this operation.

1. In the **Backups** column of a server, click the number. The backup list is displayed.
2. In the **Operation** column of a backup, click **Delete**. The backup deletion dialog box is displayed.
3. Confirm the backup information and click **OK**.

6.3.7 Managing Server Backup

Scenarios

After ransomware backup is enabled for a server, the backup vault backs up the server periodically based on a backup policy. If HSS detects a ransomware attack, the vault will back up the server immediately.

- If no backup policy is bound to the vault, it cannot perform periodic backups. You need to perform the operations in **Binding to a Backup Policy**.
- If the vault capacity is insufficient, backup cannot be performed. In this case, perform the operations in **Increasing the Backup Capacity**.
- If the backup period and backup retention rule of a backup policy do not meet your requirements, perform the operations in **Modifying a Backup Policy**.

Prerequisites

Ransomware backup has been enabled. For details, see **Enabling Backup**.

Binding to a Backup Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Prevention** > **Ransomware Prevention**.

Step 3 In the **Backup Policy Status** column of a server, click **Bind Backup Policy**.

Step 4 In the **Backup Policy** drop-down list, select a policy.

If no backup policies are available or you want to create a backup policy for the vault, click **Create Policy in CBR**. After the backup policy is created, return to the HSS console and select the new policy.

Step 5 Click **OK**.

If the **Backup Policy Status** of the server is **Enabled** and the policy name is the one you selected, the backup policy has been bound.

----End

Increasing the Backup Capacity

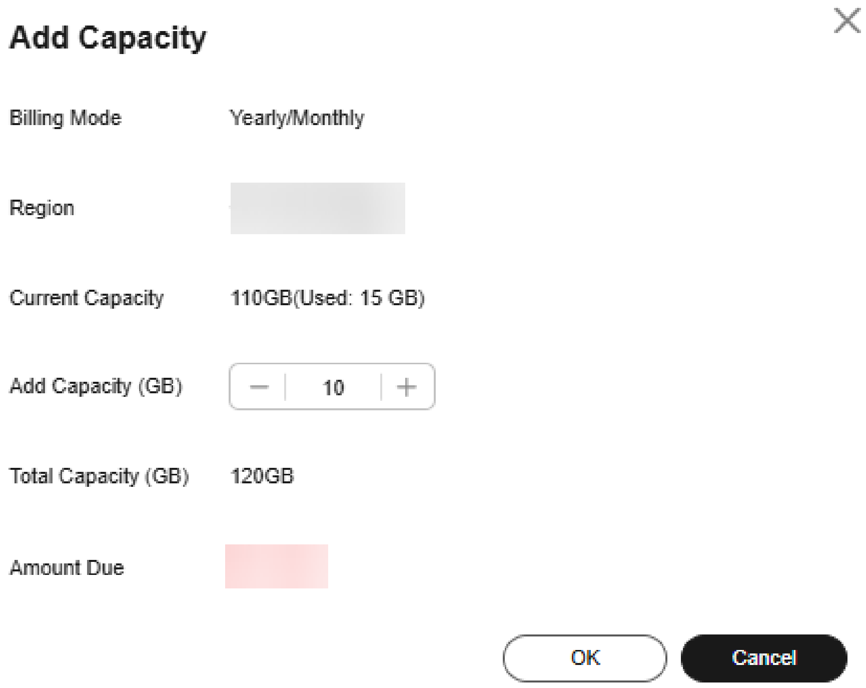
Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Server Protection** > **Ransomware Prevention**.

Step 3 Click **Add Capacity** in the **Operation** column of a server.

Step 4 In the displayed dialog box, configure the capacity.

Figure 6-34 Configuring the capacity



Add Capacity

Billing Mode	Yearly/Monthly
Region	
Current Capacity	110GB(Used: 15 GB)
Add Capacity (GB)	10
Total Capacity (GB)	120GB
Amount Due	

Step 5 If the information is correct, click **OK**. The payment page is displayed. After the payment is complete, return to the **Protected Server** tab page to view the storage capacity of the target server.

If the payment is not complete, the **Vault Status** of the target server is **Locked**. After the payment, the status becomes normal.

----End

Modifying a Backup Policy

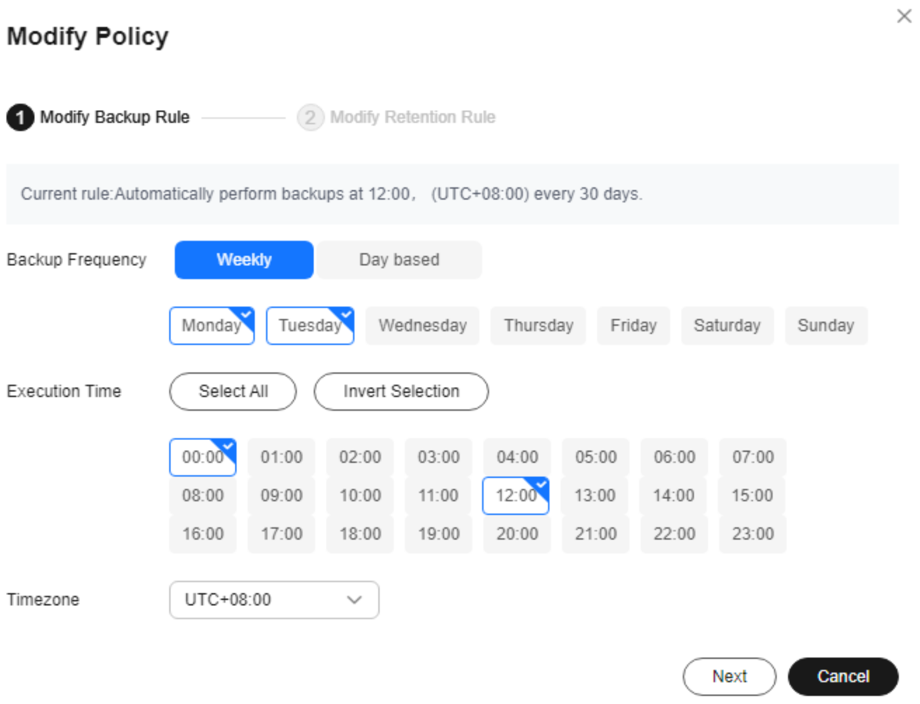
Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Server Protection** > **Ransomware Prevention**.

Step 3 Click the policy name in the **Backup Policy Status** column of a server. The **Modify Policy** dialog box is displayed.

Step 4 In the dialog box, modify the backup rule. For details, see **Policy parameters**.

Figure 6-35 Modifying a backup rule



Modify Policy

1 Modify Backup Rule —— 2 Modify Retention Rule

Current rule:Automatically perform backups at 12:00， (UTC+08:00) every 30 days.

Backup Frequency: Weekly (selected) | Day based

Monday ✓ | Tuesday ✓ | Wednesday | Thursday | Friday | Saturday | Sunday

Execution Time: Select All | Invert Selection

00:00 ✓	01:00	02:00	03:00	04:00	05:00	06:00	07:00
08:00	09:00	10:00	11:00	12:00 ✓	13:00	14:00	15:00
16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00

Timezone: UTC+08:00

Next | Cancel

Table 6-27 Parameters for modifying a backup rule

Parameter	Description	Example Value
Backup Frequency	Data can be automatically backed up on specific days in a week, or at a fixed interval. ● **Weekly**: Specifies on which days of each week the backup will be executed. You can select multiple days. ● **Day based**: Specifies the interval (every 1 to 30 days) for executing the backup. If you select **Day based**, the first backup time is supposed to be on the day when the backup policy is created. If the execution time on the day you create the backup policy has passed, the first backup will be executed in the next backup cycle.	Every 1 day

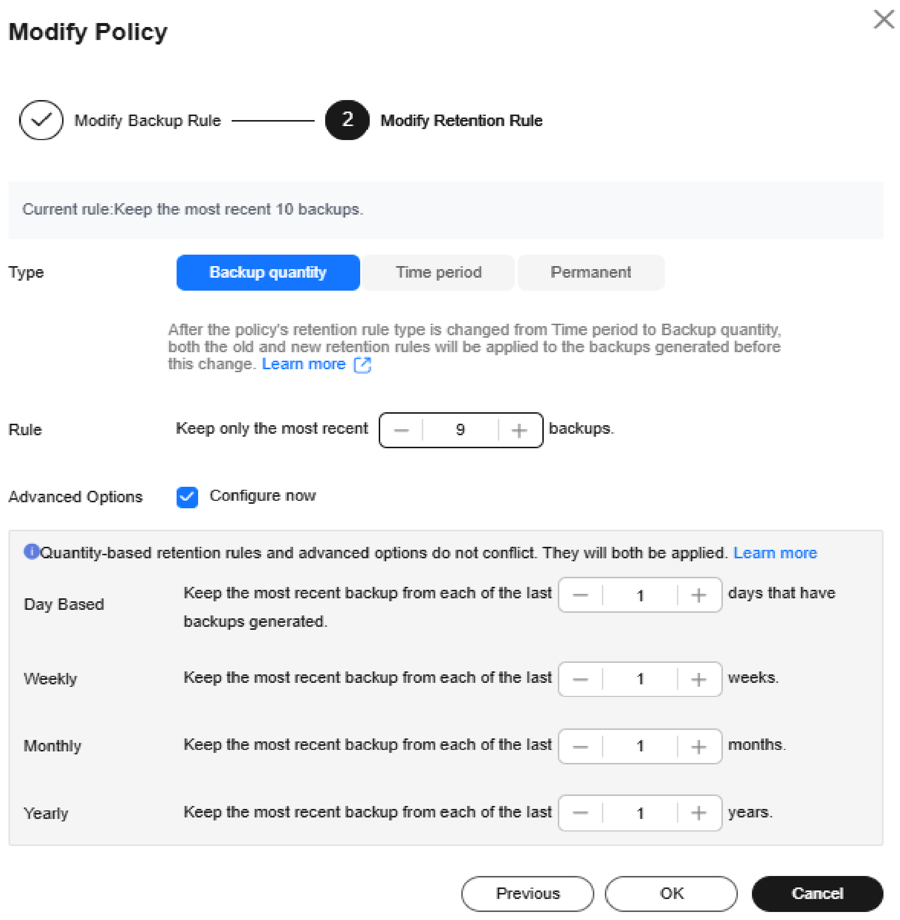
Parameter	Description	Example Value
Execution Time	Time when a backup task is executed. Backups can only be scheduled on the hour. You can select multiple hours. It is recommended that backups be performed during off-peak hours or when no services are running. Backup rule examples: ● Rule 1: Set **Backup Frequency** to **Weekly** (**Wednesday** and **Saturday**) and **Execution Time** to **00:00** and **13:00**. The backup task will be executed at 00:00 and 13:00 every Wednesday and Saturday. ● Rule 2: Set **Backup Frequency** to **Day based** and set the interval to two days. Set **Execution Time** to **02:00** and **14:00**. The backup task will be executed at 02:00 and 14:00 every two days from the date when the backup rule is set.	00:00, 07:00
Timezone	Select the time zone of the backup time.	UTC+08:00

Step 5 Confirm the settings and click **Next**. Configure the backup retention rule.

- **Type**: **Backup quantity**

  Table 6-28 describes the parameters for configuring a backup rule.

Figure 6-36 Configuring retention rules by quantity


Modify Policy

✓ Modify Backup Rule — 2 Modify Retention Rule

Current rule:Keep the most recent 10 backups.

Type: **Backup quantity** | Time period | Permanent

After the policy's retention rule type is changed from Time period to Backup quantity, both the old and new retention rules will be applied to the backups generated before this change. Learn more

Rule: Keep only the most recent − 9 + backups.

Advanced Options: ☑ Configure now

Quantity-based retention rules and advanced options do not conflict. They will both be applied. Learn more

Day Based: Keep the most recent backup from each of the last − 1 + days that have backups generated.

Weekly: Keep the most recent backup from each of the last − 1 + weeks.

Monthly: Keep the most recent backup from each of the last − 1 + months.

Yearly: Keep the most recent backup from each of the last − 1 + years.

Table 6-28 Parameters for data retention by quantity

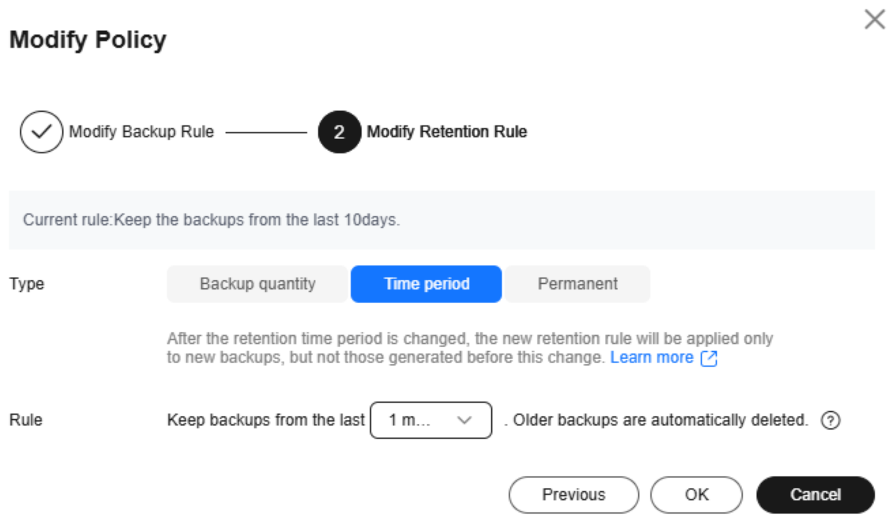
Parameter	Description	Example Value
Rule	The total number of backups retained for a single cloud server. The value range is 2 to 99,999. This setting takes effect no matter how you configure advanced options. For example, if the rule is configured to keep the most recent 30 backups, and **Advanced Options** are configured to keep the latest backups in the last 3 months (90 days), the latest 30 backups will be retained.	30

Parameter	Description	Example Value
(Optional) Advanced Options	Long-term retention rule. This rule and the quantity-based backup retention rules do not conflict. They will both be applied. – **Daily Based**: The latest backup from each of the last N days is retained. N ranges from 0 to 100. – **Weekly**: The latest backup from each of the last M weeks is retained. M ranges from 0 to 100. – **Monthly**: The latest backup from each of the last P months is retained. P ranges from 0 to 100. – **Yearly**: The latest backup from each of the last Q years is retained. Q ranges from 0 to 100.	Keep the most recent backup from each of the last three months

- **Type**: **Time period**

  Table 6-29 describes the parameters for configuring a backup rule.

Figure 6-37 Configuring retention rules by time period



Modify Policy

Current rule:Keep the backups from the last 10days.

Type: Backup quantity | Time period | Permanent

After the retention time period is changed, the new retention rule will be applied only to new backups, but not those generated before this change. Learn more

Rule: Keep backups from the last 1 m... . Older backups are automatically deleted.

Table 6-29 Parameters for data retention by time period

Parameter	Description	Example Value
Rule	You can set the backup retention period to 1 month, 3 months, 6 months, 1 year, or a custom period. The custom retention period ranges from 2 to 99,999 days. If the retention period of a backup exceeds the specified period, the backup will be automatically deleted.	3 months

- **Type**: **Permanent**

  Backup data will be permanently stored.

  NOTE

  If the **Retention Type** of a rule is changed from **Time period** to another, historical backups will still be deleted based on the **Time period** settings. For details, see **Why Does the Retention Rule Not Take Effect After Being Modified?**

Step 6 Click **OK**.

----End

6.3.8 Disabling Ransomware Prevention

Scenario

You can disable ransomware protection as needed. After protection is disabled, your server may be intruded by ransomware. Exercise caution when performing this operation.

Disabling Ransomware Prevention

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

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

Step 3 In the navigation pane, choose **Server Protection** > **Ransomware Prevention**. Click the **Protected Servers** tab.

Step 4 Choose **More** > **Disable Protection** in the **Operation** column of the target server.

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

----End

Follow-up Procedure

After ransomware prevention is disabled, the backup vault continues to back up data. If the server no longer needs backup, you can unbind from the vault in CBR.

For details, see **Dissociating Resources from a Vault**. If you no longer need the vault, you can delete it from CBR. For details, see **Deleting a Vault**.

6.4 Application Process Control

6.4.1 Application Process Control Overview

What Is Application Process Control?

Application process control helps to enhance the security of applications and processes running on servers. It can automatically identify and analyze application processes, and classify them into trusted, suspicious, and malicious processes. It allows trusted processes to run, and generates alarms for suspicious and malicious processes. This helps to build a secure environment for application processes, and protects servers from untrusted or malicious application processes.

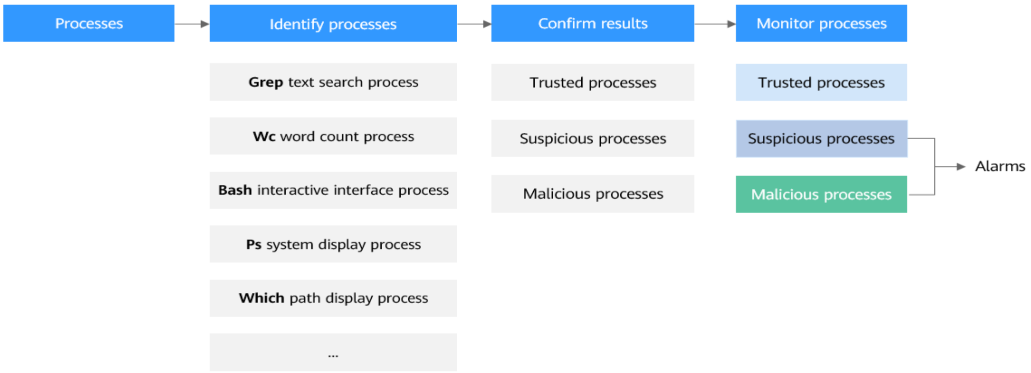
Application Process Control Principles

Application process control analyzes information in multiple dimensions, including process names, behaviors, paths, and reputation databases, to comprehensively identify processes and discover the processes disguised through renaming or obfuscation. After the processes are identified, application process control allows trusted processes (whitelisted processes) to run and generates alarms for untrusted processes. It also provides the names, hashes, file paths, occurrence time (startup time), and other important information about untrusted processes to help you perform source tracing analysis.

NOTE

Untrusted processes are probably new normal processes or infected malicious processes. If an alarm was generated for a normal process, you can add the process to the whitelist. If an alarm was generated for a malicious process, manually handle it in a timely manner.

Figure 6-38 Process of application process control



Scenarios

In a cloud server environment, the number and types of processes are usually stable. You can use the application process control function to monitor and manage process statuses and effectively identify suspicious or malicious processes, thereby building a more secure service operation environment.

Constraints

- Application process control is available only in HSS premium, WTP, and container editions. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.
- To use application process control, ensure the agent installed on the server falls within the following range. For details about how to upgrade the agent, see **Upgrading the Agent**.
  - Linux: 3.2.7 or later
  - Windows: 4.0.19 or later

Process of Using Application Process Control

Figure 6-39 Usage process

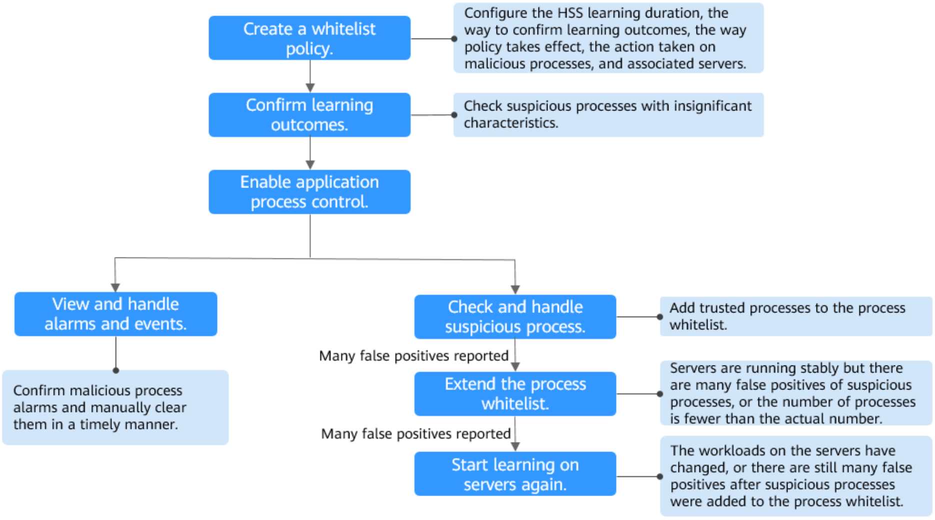

Create a whitelist policy.
Configure the HSS learning duration, the way to confirm learning outcomes, the way policy takes effect, the action taken on malicious processes, and associated servers.
Confirm learning outcomes.
Check suspicious processes with insignificant characteristics.
Enable application process control.
View and handle alarms and events.
Confirm malicious process alarms and manually clear them in a timely manner.
Check and handle suspicious process.
Add trusted processes to the process whitelist.
Many false positives reported
Extend the process whitelist.
Servers are running stably but there are many false positives of suspicious processes, or the number of processes is fewer than the actual number.
Many false positives reported
Start learning on servers again.
The workloads on the servers have changed, or there are still many false positives after suspicious processes were added to the process whitelist.

Table 6-30 Process of using application process control

Operation	Description
Create a whitelist policy.	A whitelist policy specifies how HSS learns server behaviors and protect application processes. Application process protection can be enabled only for servers associated with a whitelist policy.
Confirm learning outcomes.	After the HSS learns the application processes on servers, there may be some suspicious application processes with insignificant characteristics, and HSS cannot determine whether they are malicious or trustworthy. In this case, you need to confirm the learning outcomes.

Operation	Description
Enable application process control.	Enable application process control on the servers associated with a policy.
Check and handle suspicious processes.	HSS cannot determine whether some suspicious application processes with insignificant characteristics are trustworthy. You need to check their process details, determine whether they are trustworthy, and add them to the process whitelist.
Check and handle malicious process alarms.	HSS reports an alarm once it detects a malicious process. Choose **Detection & Response** > **Alarms**, check and handle the alarms on the **Server Alarms** tab page, and clear malicious processes in a timely manner.
(Optional) **Add items to the process whitelist.**	After HSS completes learning, if you think the number of application processes it learned is fewer than the number of process fingerprints collected by the asset fingerprint function, or if it regarded many trustworthy application processes as suspicious, you can extend the HSS process whitelist. HSS will compare the application processes it already learned with the collected process fingerprints to enrich the HSS application process intelligence library and extend the trusted process whitelist.
(Optional) **Start learning on the servers again.**	If you have added trustworthy processes to the whitelist but there are still many false positives reported, you can let HSS start learning again on the servers.

6.4.2 Creating a Whitelist Policy

Scenarios

Before enabling application process control, you need to create a whitelist policy and configure the HSS learning duration, the way to confirm learning outcomes, the way policy takes effect, and the action taken on malicious processes. HSS will manage application processes based on your policies.

Creating a Whitelist Policy

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

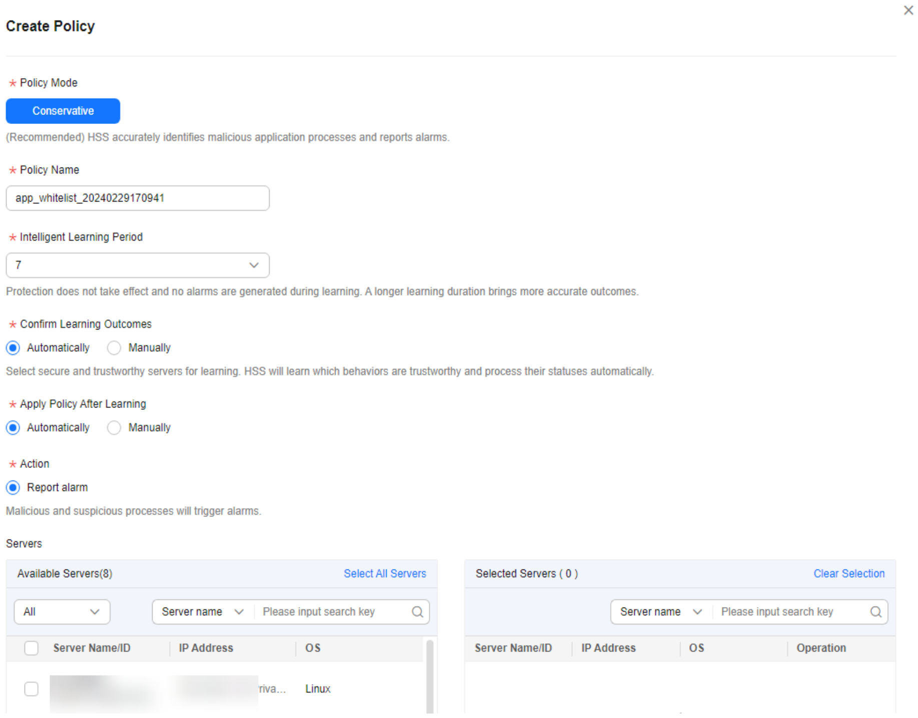
Step 2 In the upper left corner of the page, select a region, click ≡, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab. Click **Create Policy**.

Step 5 In the **Create Policy** dialog box, configure policy parameters. For details about related parameters, see **Table 6-31**.

Figure 6-40 Creating a whitelist policy



Create Policy

* Policy Mode

(Recommended) HSS accurately identifies malicious application processes and reports alarms.

* Policy Name

app_whitelist_20240229170941

* Intelligent Learning Period

7

Protection does not take effect and no alarms are generated during learning. A longer learning duration brings more accurate outcomes.

* Confirm Learning Outcomes

● Automatically ○ Manually

Select secure and trustworthy servers for learning. HSS will learn which behaviors are trustworthy and process their statuses automatically.

* Apply Policy After Learning

● Automatically ○ Manually

* Action

● Report alarm

Malicious and suspicious processes will trigger alarms.

Servers

Available Servers(8) — Select All Servers

□	Server Name/ID	IP Address	OS
□	[redacted]	[redacted] riva...	Linux

Selected Servers (0) — Clear Selection

Server Name/ID	IP Address	OS	Operation

Table 6-31 Whitelist policy parameters

Parameter	Description	Example Value
Policy Mode	Mode of the application process control policy. The conservative mode is used by default. Trustworthy and suspicious processes are allowed to run. Alarms are generated only for malicious processes.	-
Policy Name	A whitelist policy name is generated by default. You are advised to set a custom name to facilitate management.	test
Intelligent Learning Period	Number of days that HSS learns the application processes on servers. A long learning period indicates accurate learning outcomes.	7

Parameter	Description	Example Value
Confirm Learning Outcomes	The way to confirm suspicious processes with insignificant characteristics after HSS completes learning on the servers associated with the policy. ● **Automatically**: HSS automatically marks suspicious application processes with insignificant characteristics based on the application process signature database. ● **Manually**: After HSS finishes learning based on policy configurations, choose **Application Process Control** > **Whitelist Policies**. Click a policy name. On the policy details page, click the **Process Files** tab and filter processes in the **To be confirmed** state. Manually mark suspicious processes with insignificant characteristics.	Automatically
Apply Policy After Learning	The way application process control is enabled after HSS completes learning on the servers associated with the policy. ● **Automatically**: Application process control is automatically enabled after HSS completes learning on the servers associated with the policy. ● **Manually**: Manually enable application process control as needed after HSS completes learning. For more information, see **Enabling Application Process Control**.	Automatically
Action	Action taken when a malicious process is detected. Alarms are generated for malicious processes.	Report alarm
Servers	Servers to be protected. The agent version falls within the following scope. For details about how to upgrade the agent, see **Viewing Server Protection Status**.	-

Step 6 Click **OK**.

You can view the created policy and its status in the policy list. For more information, see **Table 6-32**.

Table 6-32 Policy status description

Policy Status	Description
Learning	HSS is learning the characteristics of the application processes on servers. Please wait.
Learning complete but not in effect	The server characteristics associated with the policy have been learned. Confirm the learning outcomes. For details, see **Confirming Learning Outcomes**.

Policy Status	Description
Learning complete and in effect	Application process control protection has been enabled for servers.

----End

Related Operations

Editing a whitelist policy

You can modify the policy mode, action, or protected servers in a whitelist policy.

Step 1 In the row of a policy, click **Edit** in the **Operation** column.

Step 2 In the **Edit Policy** dialog box, modify parameters and click **OK**.

----End

Deleting a whitelist policy

If you no longer need HSS to provide application process control for the servers associated with a policy and do not need to retain the application process information learned by HSS, you can delete the whitelist policy. If you need to enable application process control for the servers after the deletion, HSS will need to start learning again. Exercise caution when performing this operation.

Step 1 In the row of a policy, click **Delete** in the **Operation** column.

Step 2 In the displayed dialog box, click **OK**.

----End

6.4.3 Confirming Learning Outcomes

Scenarios

After HSS completes learning on the servers associated with a whitelist, there may be some suspicious processes with insignificant characteristics that need to be confirmed. You can manually or let HSS automatically mark them as suspicious, malicious, or trusted processes.

You can configure how to confirm learning outcomes only when **creating a whitelist policy**. The value of **Confirm Learning Outcomes** can be:

- **Automatically**: Suspicious processes are automatically marked based on the application process intelligence.
- **Manually**: You need to manually check and mark suspicious processes. This section describes the detailed procedure.

Prerequisites

A policy has been created and its status is **Learning complete but not in effect**. For details, see **Creating a Whitelist Policy**.

Confirming Learning Outcomes

Step 1 Log in to the management console.

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

Step 3 In the navigation tree, choose **Server Protection** > **Application Process Control**.

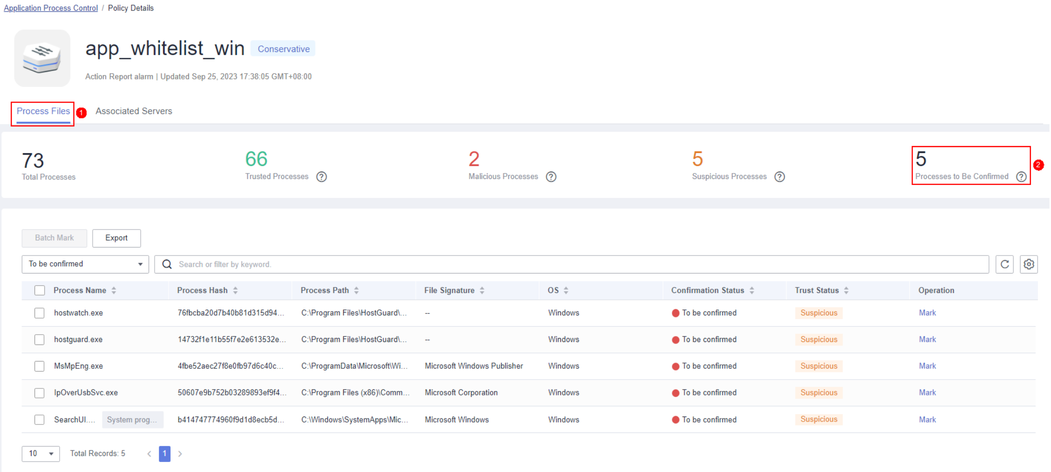
Step 4 Click the **Whitelist Policies** tab.

Step 5 Click the name of a policy whose **Policy Status** is **Learning complete but not in effect**. The **Policy Details** page is displayed.

Step 6 Click the **Process Files** tab.

Step 7 Click the number of processes to be confirmed.

Figure 6-41 Viewing processes to be confirmed



Application Process Control / Policy Details

app_whitelist_win Conservative

Action Report alarm | Updated Sep 25, 2023 17:38:05 GMT+08:00

Process Name	Process Hash	Process Path	File Signature	OS	Confirmation Status	Trust Status	Operation
hostwatch.exe	76fbcba20d7b40b81d315d94...	C:\Program Files\HostGuard\...	--	Windows	● To be confirmed	Suspicious	Mark
hostguard.exe	14732f1e11b55f7e2e613532e...	C:\Program Files\HostGuard\...	--	Windows	● To be confirmed	Suspicious	Mark
MsMpEng.exe	4fbe52aec27f8e0fb97d6c40c...	C:\ProgramData\Microsoft\Wi...	Microsoft Windows Publisher	Windows	● To be confirmed	Suspicious	Mark
IpOverUsbSvc.exe	50607e9b752b03289893ef9f4...	C:\Program Files (x86)\Comm...	Microsoft Corporation	Windows	● To be confirmed	Suspicious	Mark
SearchUI.... System prog...	b414747774960f9d1d8ecb5d...	C:\Windows\SystemApps\Mic...	Microsoft Windows	Windows	● To be confirmed	Suspicious	Mark

Step 8 Check whether the application processes are trustworthy based on their names and file paths.

Step 9 In the row of a process, click **Mark** in the **Operation** column.

You can also select all application processes and click **Batch Mark** above the process list.

Step 10 In the **Mark** dialog box, set **Trust Status**.

Select **Suspicious**, **Trusted**, or **Malicious**.

Step 11 Click **OK**.

----End

Follow-up Operations

After the learning outcomes are confirmed, you can enable application process protection. For details, see **Enabling Application Process Control**.

6.4.4 Enabling Application Process Control

Scenarios

HSS can control different types of application processes on servers. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes.

You can configure how to enable application process control when **creating a whitelist policy**. The value of **Apply Policy After Learning** can be:

- **Automatically**: Application process control is automatically enabled after HSS completes learning on the servers associated with the policy.
- **Manually**: Manually enable application process control as needed after HSS completes learning. This section describes the detailed procedure.

Prerequisites

A whitelist policy has been created and the policy learning outcomes have been confirmed. For details, see **Creating a Whitelist Policy** and **Confirming Learning Outcomes**.

Enabling Application Process Control

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

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

Step 3 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab.

Step 5 In the **Operation** column of a policy, click **Enable Protection**.

You can also select multiple policies and click **Enable Protection** above the policy list.

Step 6 In the **Enable Protection** dialog box, click **OK**.

Step 7 Check the policy status. If **Policy Status** is **Learning complete and in effect**, application protection has been enabled.

----End

Follow-up Operations

After application process control protection is enabled, alarms will be reported for suspicious and malicious processes running on servers.

- For details about how to handle running suspicious processes, see **Checking and Handling Suspicious Processes**.
- For details about how to handle running malicious processes, see **Handling Server Alarms**.

6.4.5 Checking and Handling Suspicious Processes

Scenarios

If a new application process is started after application process control was enabled, HSS will display it in the suspicious process list. In this case, determine whether the process can be trusted. If it is a normal process, add it to the process whitelist.

Checking and Handling Suspicious Processes

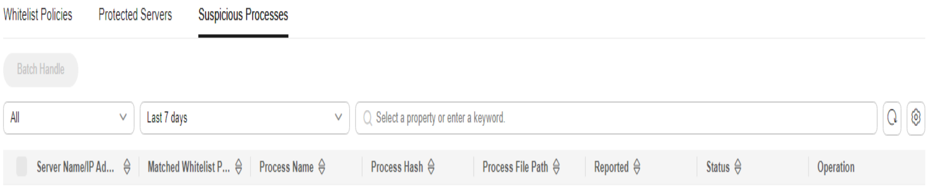
Step 1 Log in to the management console.

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

Step 3 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 4 Click the **Suspicious Processes** tab.

Figure 6-42 Viewing suspicious processes



Step 5 Determine whether a suspicious process can be trusted based on its information, such as the hash value and file path.

- If the process can be trusted, go to **Step 6**.
- If the process cannot be trusted, manually clear it.

Step 6 In the row of a process, click **Handle** in the **Operation** column.

You can also select multiple suspicious processes and click **Batch Handle** above the list.

Step 7 In the dialog box that is displayed, select an action.

Select **Add to process whitelist**.

Step 8 Click **OK**.

----End

Related Operations

HSS reports an alarm once it detects a malicious process. Choose **Detection & Response** > **Alarms**, check and handle the alarms on the **Server Alarms** tab page, and clear malicious processes in a timely manner. For details, see **Handling Server Alarms**.

6.4.6 Extending the Process Whitelist

Scenarios

After HSS completes learning the whitelist policy, if you think the number of application processes it learned is fewer than the number of process fingerprints collected by the asset fingerprint function, or if it regarded many trustworthy application processes as suspicious, you can extend the process whitelist. HSS will compare the application processes it already learned with the collected process fingerprints to enrich the HSS application process intelligence library and extend the trusted process whitelist.

For details about how to confirm the learning results of the application process whitelist, see **Confirming Learning Outcomes**. For details about how to view the process fingerprints, see **Viewing Server Asset Fingerprints**.

Extending the Process Whitelist

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

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

Step 3 In the navigation tree, choose **Server Protection** > **Application Process Control**.

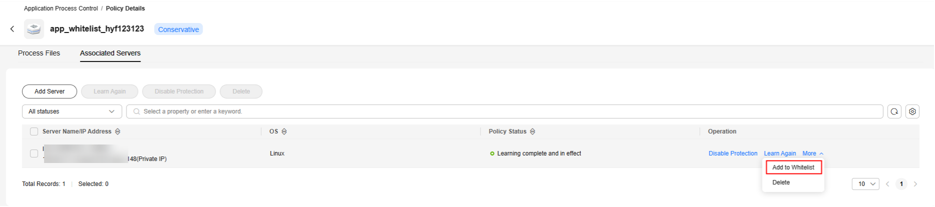
Step 4 Click the **Whitelist Policies** tab.

Step 5 Click a policy name. The **Policy Details** page is displayed.

Step 6 Click the **Associated Servers** tab.

Step 7 In the row of a server, choose **More** > **Add to Whitelist** in the **Operation** column.

Figure 6-43 Extending the process whitelist



Server Name/IP Address	OS	Policy Status	Operation
[redacted] 148(Private IP)	Linux	Learning complete and in effect	Disable Protection Learn Again More

Total Records: 1 | Selected: 0

Step 8 Click **Compare** to compare the server process fingerprints with the application processes learned by the whitelist.

Step 9 Select trusted processes and click **Add**.

Click the **Process Files** tab.

----End

6.4.7 Start Learning on Servers Again

Scenarios

If you have **extended the process whitelist** but there are still many false positives reported, or if your server workloads changed, you can let HSS start learning again on the servers and calibrate its application process intelligence library to reduce false positives.

Start Learning on Servers Again

Step 1 Log in to the management console.

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

Step 3 In the navigation tree, choose **Server Protection** > **Application Process Control**.

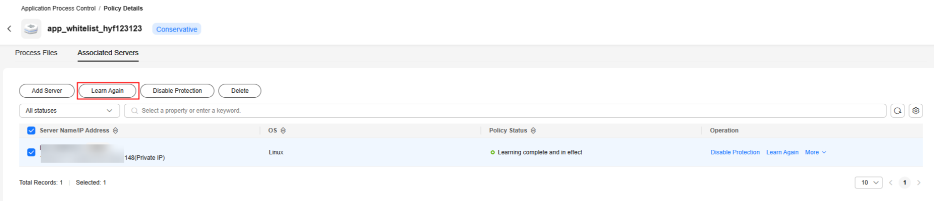
Step 4 Click the **Whitelist Policies** tab.

Step 5 Click a policy name. The **Policy Details** page is displayed.

Step 6 Click the **Associated Servers** tab.

Step 7 Select servers and click **Learn Again** above the list.

Figure 6-44 Start learning on servers again



☑ Server Name/IP Address	OS	Policy Status	Operation
☑ [redacted]148(Private IP)	Linux	○ Learning complete and in effect	Disable Protection Learn Again More

Total Records: 1 | Selected: 1

Step 8 In the dialog box that is displayed, click **OK**.

The relearning is performed according to the intelligent learning time specified in the policy. After the learning is complete, confirm the learning results in a timely manner. For details, see **Confirming Learning Outcomes**.

----End

6.4.8 Disabling Application Process Control

Scenarios

You can disable application process control for one or multiple servers at a time.

Disabling Protection for Servers Associated with a Policy

Step 1 Log in to the management console.

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

Step 3 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab.

Step 5 Disable application process control.

- Disable protection but retain the application process characteristics learned by HSS.

   a. In the **Operation** column of a policy, click **Disable Protection**. Alternatively, select multiple policies and click **Disable** above the policy list.
   b. Click **OK**.

- Disable protection and delete the application process characteristics learned by HSS.
   a. In the row of a policy, click **Delete** in the **Operation** column.
   b. Click **OK**.

Step 6 Check the policy list.

- Disable protection but retain the application process characteristics learned by HSS.

  If the **Policy Status** of the policy is **Learning complete but not in effect**, application process control has been disabled.

- Disable protection and delete the application process characteristics learned by HSS.

  If the policy is deleted from the policy list, application process control has been disabled.

----End

Disabling Protection for a Single Server

Step 1 Log in to the management console.

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

Step 3 In the navigation tree, choose **Server Protection** > **Application Process Control**.

Step 4 Click the **Whitelist Policies** tab.

Step 5 Click a policy name. The **Policy Details** page is displayed.

Step 6 Click the **Associated Servers** tab.

Step 7 Disable application process control.

- Disable protection but retain the association between the server and the policy.
   a. In the **Operation** column of a policy, click **Disable Protection**. Alternatively, select multiple policies and click **Disable** above the policy list.
   b. Click **OK**.
- Disable protection and disassociate the server from the policy.

  NOTE

  To change the protection policy associated with a server, remove the server from the policy settings, and then create or edit another protection policy to associate with the server.

   a. In the row containing the desired instance, click **Delete** in the **Operation** column.

b. Click **OK**.

Step 8 Check the server list.

- Disable protection but retain the association between the server and the policy.

  If the **Policy Status** of the server is **Learning complete but not in effect**, application process control has been disabled.

- Disable protection and disassociate the server from the policy.

  If the server is deleted from the list, application process control has been disabled.

----End

6.5 File Integrity Monitoring

6.5.1 File Integrity Management Overview

File integrity management (FIM) monitors key files on Linux servers in real time; records file addition, modification, and deletion; and reports alarms, helping you detect suspicious changes in a timely manner.

File Integrity Monitoring Principles

HSS checks for suspicious changes by comparing the previous and current statuses of a file.

File Integrity Monitoring Scope

Some file monitoring paths are preconfigured in HSS. For details, see **Table 6-33**.

To add or remove monitored files, you can modify parameters in the **File Integrity** area in the **File Protection** policy. For details, see **Configuring Policies**.

Table 6-33 Default file monitoring paths

Type	File Path
bin	● /bin/ls ● /bin/ps ● /bin/bash ● /bin/login

Type	File Path
usr	● /usr/bin/ls ● /usr/bin/ps ● /usr/bin/bash ● /usr/bin/login ● /usr/bin/passwd ● /usr/bin/top ● /usr/bin/killall ● /usr/bin/ssh ● /usr/bin/wget ● /usr/bin/curl

Constraints

- File integrity management is available in HSS professional, enterprise, premium, WTP, and container editions. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.
- File integrity management applies only to Linux servers.

6.5.2 Viewing File Change Records

File integrity monitoring provides change statistics, change types, and file change records, helping you learn about file changes in real time and detect malicious changes in a timely manner.

Viewing File Change Overview

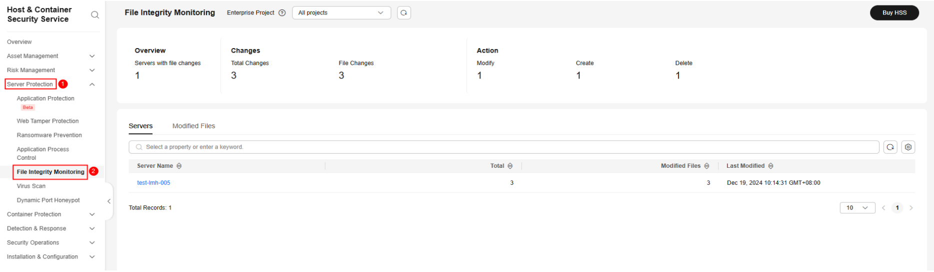
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane, choose **Server Protection** > **File Integrity Monitoring**. Check the file change overview.

You can select an enterprise project for filtering.

Figure 6-45 File integrity monitoring page



File Integrity Monitoring Enterprise Project: All projects

Overview: Servers with file changes 1

Changes: Total Changes 3; File Changes 3

Action: Modify 1; Create 1; Delete 1

Server Name	Total	Modified Files	Last Modified
test-lmh-005	3	3	Dec 19, 2024 10:14:31 GMT+08:00

Total Records: 1

Table 6-34 File change overview parameters

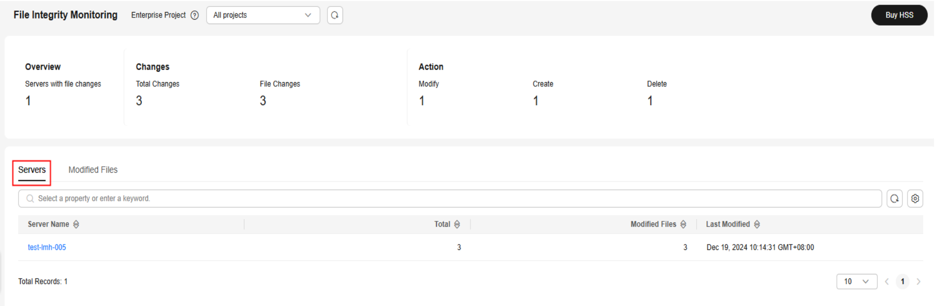
Parameter	Description
Overview	Number of servers where files are changed.
Changes	● **Total Changes**: total number of file changes. ● **File Changes**: total number of file changes.
Action	● **Modify**: total number of file changes. ● **Create**: total number of file creations. ● **Delete**: total number of file deletions.

----End

Viewing the File Change Records of a Single Server

Step 1 In the server list, you can view the number of files and registry changes on a servers and the time when they were last changed.

Figure 6-46 Server list



File Integrity Monitoring
Enterprise Project
All projects
Buy HSS
Servers
Modified Files
Select a property or enter a keyword.

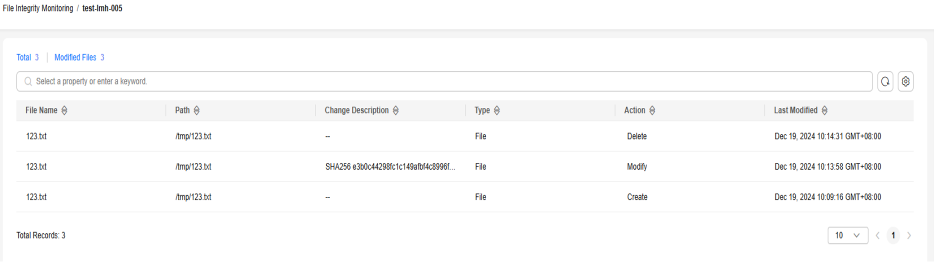
Overview	Changes		Action		
Servers with file changes	Total Changes	File Changes	Modify	Create	Delete
1	3	3	1	1	1

Server Name	Total	Modified Files	Last Modified
test-lmh-005	3	3	Dec 19, 2024 10:14:31 GMT+08:00

Total Records: 1

Step 2 Click a server name to go to the server change details page. You can view the file change details of the server.

Figure 6-47 Viewing file change records on a server



File Integrity Monitoring / test-lmh-005
Total 3
Modified Files 3
Select a property or enter a keyword.

File Name	Path	Change Description	Type	Action	Last Modified
123.txt	/tmp/123.txt	--	File	Delete	Dec 19, 2024 10:14:31 GMT+08:00
123.txt	/tmp/123.txt	SHA256 e3b0c44298fc1c149afbf4c8996f...	File	Modify	Dec 19, 2024 10:13:58 GMT+08:00
123.txt	/tmp/123.txt	--	File	Create	Dec 19, 2024 10:09:16 GMT+08:00

Total Records: 3

Table 6-35 Server file change parameters

Parameter	Description	Example Value
File Name	Name of a modified file.	du
Path	Path of a modified file.	-

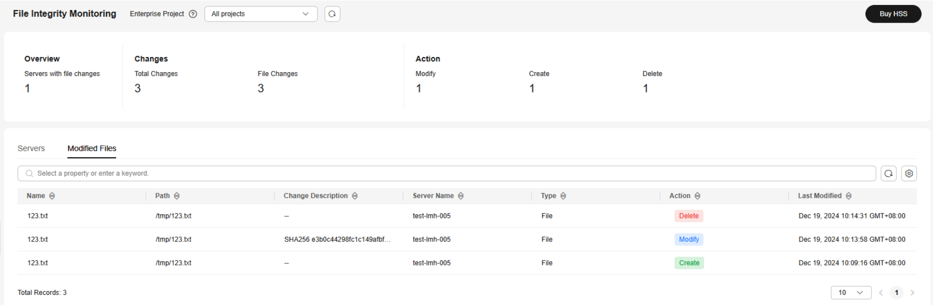
Parameter	Description	Example Value
Change Description	Description of the change. To view the change details, hover the cursor over the change content.	-
Type	File	File
Action	How a file was modified. ● Create ● Modify ● Delete	Modify
Last Modified	The last time when a file was modified.	-

----End

Viewing the File Change Records of All Servers

In the modified file list, you can view all file change records. For details, see **Table 6-35**.

Figure 6-48 Checking modified files


File Integrity Monitoring
Enterprise Project
All projects
Buy HSS
Servers
Modified Files
Select a property or enter a keyword.

Overview
Servers with file changes
1

Changes
Total Changes 3
File Changes 3

Action
Modify 1
Create 1
Delete 1

Name	Path	Change Description	Server Name	Type	Action	Last Modified
123.txt	/tmp/123.txt	--	test-lmh-005	File	Delete	Dec 19, 2024 10:14:31 GMT+08:00
123.txt	/tmp/123.txt	SHA256 e3b0c44298fc1c149afbf...	test-lmh-005	File	Modify	Dec 19, 2024 10:13:58 GMT+08:00
123.txt	/tmp/123.txt	--	test-lmh-005	File	Create	Dec 19, 2024 10:09:16 GMT+08:00

Total Records: 3

6.6 Virus Scan

6.6.1 Virus Scan Overview

What Is Virus Scan?

Viruses are self-replicable instructions or program codes compiled independently or embedded in server systems to adversely affect the servers by damaging their functions or data. Once a virus infiltrates a server, it can cause a range of damages – from occupying the system memory and slowing down operations to important data loss, data leaks, and system breakdown, causing immeasurable losses.

HSS can help you detect and remove viruses to protect your servers.

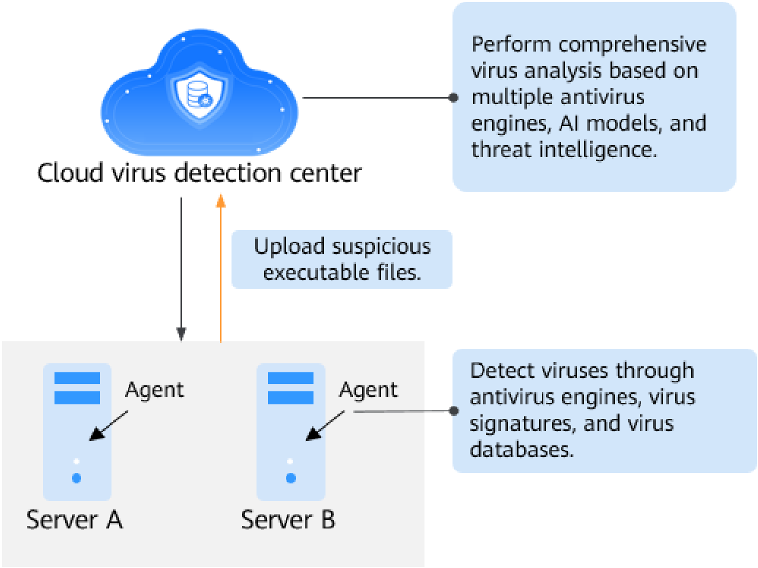
HSS combines cloud-based and local antivirus mechanisms to scan executable files, compressed files, scripts, documents, images, and audiovisual files for viruses.

You can perform quick scan, full-disk scan, and custom scans on servers as needed to detect and remove virus files in a timely manner, enhancing the virus defense of the system.

Virus Scan and Removal Principles

The HSS antivirus combines cloud-based and local antivirus mechanisms. On servers, it uses the virus signature database and agent-side antivirus engine to quickly scan all static files. A malicious file is isolated once it is detected. A suspicious executable file can be uploaded to the cloud virus detection center. This center uses multiple antivirus engines, AI models, and threat intelligence technologies to further evaluate suspicious files and remove viruses.

Figure 6-49 Virus scan and removal principles


Cloud virus detection center
Perform comprehensive virus analysis based on multiple antivirus engines, AI models, and threat intelligence.
Upload suspicious executable files.
Agent
Agent
Server A
Server B
Detect viruses through antivirus engines, virus signatures, and virus databases.

Detectable and Removable Viruses

Antivirus can scan for and remove ransomware, mining programs, DDoS Trojans, Trojan programs, backdoors, malicious programs, high-risk programs, worms, suspicious programs, and self-mutating Trojans.

Advantages of Virus Scan and Removal

- **Fast and accurate file type identification**

  This function integrates dedicated file type identification algorithms to check the real content of files and effectively detect fake file suffixes or content. Hundreds of file types can be quickly and accurately identified.

- **In-depth parsing of malicious files**

  The Cloud+Local collaborative virus detection mechanism analyzes binary files, compound documents, and diverse scripts. It can restore complete file content and deeply identify potential malicious behaviors.

- **24/7 update to the latest virus detection capabilities**

  Huawei Cloud virus analysis experts built a complete, reliable, and efficient cloud intelligent security center based on the computing technologies of the intelligence center to accurately defend against and analyze massive latest viruses in real time. HSS updates the latest protection capabilities from the security intelligence center in real time to defend against the latest viruses in a timely manner.

Constraints

- This function is available in HSS professional, enterprise, premium, WTP, and container editions. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.
  - Professional edition: quick scan and removal
  - Enterprise edition and other editions: quick, full-disk, and customized scan and removal
- To use virus scan and removal, ensure the agent installed on the server falls within the following ranges. For more information, see **Upgrading the Agent**.
  - Linux: 3.2.9 or later
  - Windows: 4.0.20 or later
- To use virus scan and removal, ensure the **AV Detection** policy is enabled. For details, see **Configuring Policies**.

Process of Virus Scan

Figure 6-50 Process of Virus Scan

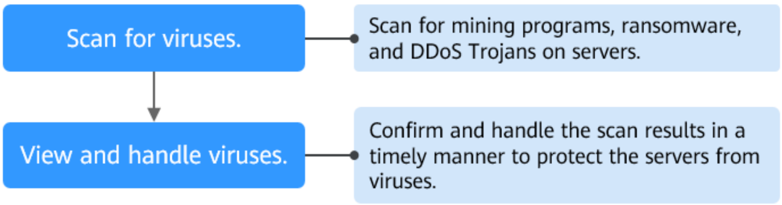

Scan for viruses.
Scan for mining programs, ransomware, and DDoS Trojans on servers.
View and handle viruses.
Confirm and handle the scan results in a timely manner to protect the servers from viruses.

Table 6-36 Virus scan and removal process

Operation	Description
Scanning for Viruses	You can perform quick scans, full scans, or custom scans to check your servers for viruses, including mining programs, ransomware, and DDoS Trojans.
Viewing and Handling Viruses	HSS allows you to isolate, remove, whitelist, or ignore virus-infected files. You can isolate and remove different types of viruses. To protect servers from viruses, you are advised to view and handle the scan results in a timely manner after the scan is complete.

6.6.2 Scanning for Viruses

Scenarios

Once a static virus file is started, it may become a malicious process and become a security risk of servers. You are advised to scan for and clear viruses on servers in a timely manner.

HSS supports quick scans, full-disk scans, and custom scans. For details, see **Table 6-37**.

Table 6-37 Virus scan methods

Method	Description	File Type	Directory Scope
Quick Scan	Quick virus scan tasks can save time and costs. This function scans and removes preset key system files and directories.	● Windows Processes (active processes, hidden processes, and Docker processes), kernel modules, installed programs, dynamic library hijacking, services, scheduled tasks, auto-started items, sensitive directories, Office files, images, videos, scripts, and compressed packages ● Linux Processes (active processes, hidden processes, and Docker processes), kernel modules, installed programs, dynamic library hijacking, services, scheduled tasks, auto-started items, sensitive directories,	● Windows – User desktop, downloaded files, and document directories – Startup items in the Start menu – System directories **C:\Windows\System**, **C:\Windows\System32**, **C:\Windows\SysWOW64** – Temporary directories **C:\Users\***[Username]***\AppData\Local\Temp\**, **C:\Temp**, **C:\Windows\Temp** – Download directories of browsers Google Chrome, Microsoft Edge, and Mozilla Firefox ● Linux – Standard system directories **/bin**, **/sbin**, **/lib**, **/lib64**, **/usr/bin**, **/usr/sbin**, **/usr/lib**, **/usr/lib64**, **/usr/local/lib**, **/usr/local/lib64**, **/usr/local/bin**, **/usr/local/sbin** – Other important directories **/tmp**, **/root**, **/home**, **/boot**, **/opt**, **/data**, **/var/tmp**, **/var/run**, **/var/lib**, **/dev/shm**, **/etc**, **/etc/sysconfig**, **/usr/local/src**, **/usr/share**, and the root directory – Directories of the executable files corresponding to the startup items **/etc/rc.d**, **/etc/init.d**

Method	Description	File Type	Directory Scope
		Office files, images, videos, scripts, and compressed packages	
Full-disk Scan	A time-consuming full-disk virus scan can comprehensively check servers for viruses.	- **Executable**: executable files and dynamic link libraries (DLLs), such as .exe, .dll, and .so files - **Compressed**: installation packages or other compressed packages, such as .zip, .rar, and .tar files - **Script**: script files, such as .bat, .py, and .ps1 files - **Document**: document files, such as .txt, .doc, and .pdf files - **Image**: image files, such as .bmp, .jpg, and .gif files - **Audio & Video**: audiovisual files, such as .mp3, .mp4, and .flv files	All directories except network directories. The reasons for not scanning network directories are as follows: 1. A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. 2. The access to network directories may occupy all your bandwidth and affect your services. You can create a custom scan task to scan network directories.
Custom Scan	You can create a custom virus scan task as needed.	You can scan executable, compressed, script, document, image, or audiovisual files.	User-defined

Constraints

- A virus scan uses a lot of memory, CPU, and I/O resources. Perform this operation during off-peak hours. For details about the resource usage, see **How Many CPU and Memory Resources Are Occupied by the Agent When It Performs Scans?**
- The HSS professional edition only supports quick scan and removal.
- A full-disk scan does not check network directories.

Quick Scan

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

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

Step 3 Choose **Server Protection** > **Virus Scan**.

Step 4 Click **Quick Scan**. The dialog box is displayed.

Step 5 Set parameters related to the quick scan task as prompted.

Table 6-38 Quick scan parameters

Parameter	Description	Example Value
Task Name	HSS automatically generates a task name based on the task creation time (accurate to seconds). You can modify it as needed.	Quick Scan-20250425173536
Select Server	Select the servers where you want to perform a quick scan. You can select and scan servers that meet all the following conditions: ● The agent is online and meets the following requirements. For details about how to install the agent, see **Installing the Agent on Servers**. – Unlimited scans: Windows agent version ≥ 4.0.20, Linux agent version ≥ 3.2.9 – Pay-per-use scans: Windows agent version ≥ 4.0.23, Linux agent version ≥ 3.2.12 ● The AV detection policy is enabled. For details about how to enable it, see **Configuring Policies**. ● The server is not being scanned.	-

Parameter	Description	Example Value
Handling Policy	Action to be taken on the detected virus-infected files. ● **Automatic Handling**: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled. **CAUTION** In rare cases, files may be incorrectly isolated. In this case, you can restore the isolated files on the **Isolated Files** page. For details, see **Restoring Isolated Files**. ● **Manual Handling**: Alarms are generated only for detected infected files. You need to manually confirm the files before handling them.	Automatic Handling

Step 6 Click **Scan** and start the scan task.

----End

Full-disk Scan

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

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

Step 3 Choose **Server Protection** > **Virus Scan**.

Step 4 Click **Full-disk Scan**. The dialog box is displayed.

Step 5 Set parameters related to the full-disk scan task as prompted.

Table 6-39 Full-disk scan parameters

Parameter	Description	Example Value
Task Name	HSS automatically generates a task name based on the task creation time (accurate to seconds). You can modify it as needed.	Full-disk Scan-20250425174038

Parameter	Description	Example Value
Select Server	Select the servers where you want to perform a full scan. You can select and scan servers that meet all the following conditions: ● The agent is online and meets the following requirements. For details about how to install the agent, see **Installing the Agent on Servers**. – Unlimited scans: Windows agent version ≥ 4.0.20, Linux agent version ≥ 3.2.9 – Pay-per-use scans: Windows agent version ≥ 4.0.23, Linux agent version ≥ 3.2.12 ● The AV detection policy is enabled. For details about how to enable it, see **Configuring Policies**. ● The server is not being scanned.	-
Handling Policy	Action to be taken on the detected virus-infected files. ● **Automatic Handling**: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled. **CAUTION** In rare cases, files may be incorrectly isolated. In this case, you can restore the isolated files on the **Isolated Files** page. For details, see **Restoring Isolated Files**. ● **Manual Handling**: Alarms are generated only for detected infected files. You need to manually confirm the files before handling them.	Automatic Handling

Step 6 Click **Scan** and start the scan task.

----End

Custom Scan

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

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

Step 3 Choose **Server Protection** > **Virus Scan**.

Step 4 Click **Custom Scan**.

Step 5 Set the parameters of the **Custom Scan** policy as prompted. For details about the parameters, see **Custom antivirus policy parameters**.

Table 6-40 Custom antivirus policy parameters

Parameter	Description	Example Value
Task Name	HSS automatically generates a task name based on the task creation time (accurate to seconds). You can modify it as needed.	Custom Scan-20250425180036
Startup Type	Scan task execution type. ● **Scan Now**: Start a scan immediately. ● **Scan Later**: Start a scan at the specified time. ● **Periodic Start**: Start a scan periodically based on your settings.	Scan Later
Start	If **Startup Type** is set to **Scan Later**, configure this parameter to set the start time of the scan. You can set the start time to a time within one month.	2025/04/25 18:10
Schedule	If **Startup Type** is set to **Periodic Start**, configure this parameter to set the scan period.	-
File Type	Type of the file to be scanned. Currently, the following types of files can be scanned: ● **Executable**: executable files and dynamic link libraries (DLLs), such as .exe, .dll, and .so files ● **Compressed**: installation packages or other compressed packages, such as .zip, .rar, and .tar files ● **Script**: script files, such as .bat, .py, and .ps1 files ● **Document**: document files, such as .txt, .doc, and .pdf files ● **Image**: image files, such as .bmp, .jpg, and .gif files ● **Audio & Video**: audiovisual files, such as .mp3, .mp4, and .flv files	Select All
(Optional) Directory Settings	Directory where virus-infected files need to be scanned. If this parameter is not set, full scan is performed by default. Full scan does not cover network directories.	-

Parameter	Description	Example Value
(Optional) Exclude Specified Directories	Directories that do not require virus scan.	-
Select Server	Select the servers to be scanned. You can select and scan servers that meet all the following conditions: ● The agent is online and meets the following requirements: For details about how to install the agent, see **Installing the Agent on Servers**. – Unlimited scans: Windows agent version ≥ 4.0.20, Linux agent version ≥ 3.2.9 – Pay-per-use scans: Windows agent version ≥ 4.0.23, Linux agent version ≥ 3.2.12 ● The AV detection policy is enabled. For details about how to enable it, see **Configuring Policies**. ● The task start conditions required by the corresponding policy are met: – Policy whose **Startup Type** is **Scan Now**: The server is not being scanned. – Policy whose **Startup Type** is **Scan Later**: No other custom scan policies using the same startup time as the current policy are bound to the server. – Policy whose **Startup Type** is **Periodic Start**: No other custom policies whose **Startup Type** is **Periodic Start** are bound to the server.	-

Parameter	Description	Example Value
Handling Policy	Action to be taken on the detected virus-infected files. ● **Automatic Handling**: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled. CAUTION In rare cases, files may be incorrectly isolated. In this case, you can restore the isolated files on the **Isolated Files** page. For details, see **Restoring Isolated Files**. ● **Manual Handling**: Alarms are generated only for detected infected files. You need to manually confirm the files before handling them.	Automatic Handling

Step 6 Click **Scan** and start the scan task.

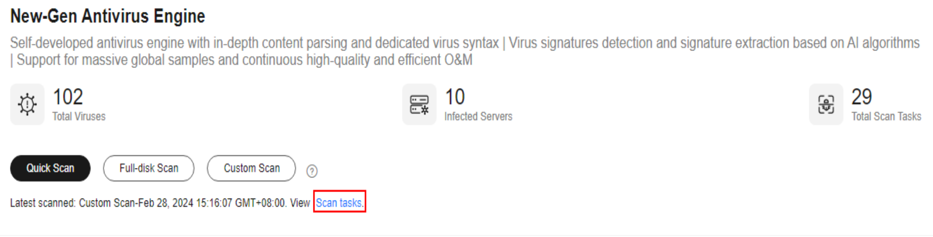
----End

Viewing Virus Scan Status

After starting a scan task, you can view its execution status by referring to this section.

Step 1 On the **Virus Scan** page, click **Scan tasks**. The **Scan Tasks** page is displayed.

Figure 6-51 Viewing scan tasks



New-Gen Antivirus Engine

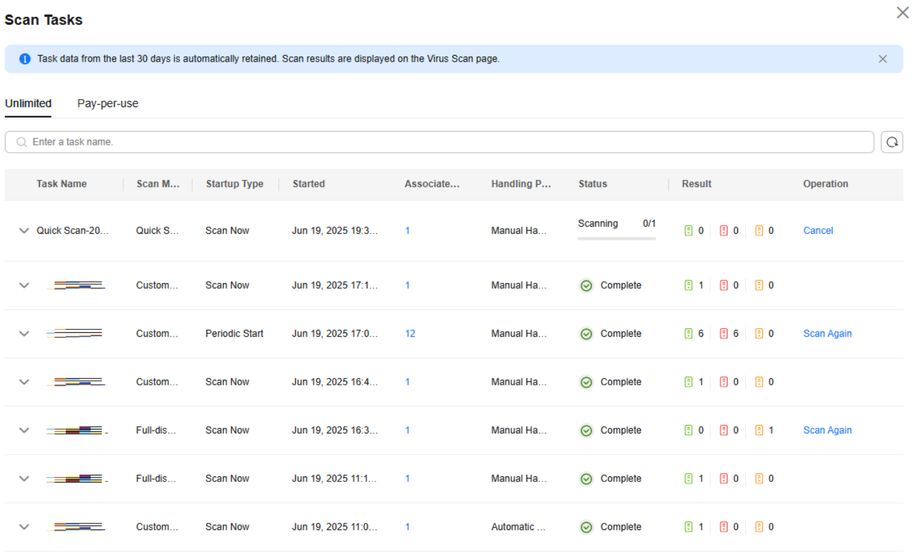
Self-developed antivirus engine with in-depth content parsing and dedicated virus syntax | Virus signatures detection and signature extraction based on AI algorithms | Support for massive global samples and continuous high-quality and efficient O&M

Latest scanned: Custom Scan-Feb 28, 2024 15:16:07 GMT+08:00. View Scan tasks.

Step 2 On the **Scan Task** page, view the task start time, task status, and scan status.

- To view information about specific scan tasks, configure search criteria in the search box above the scan task list.
- To stop an ongoing scan task, click **Cancel** in the **Operation** column of the task.
- To retry a failed scan task, click **Scan Again** in the **Operation** column of the task.

Figure 6-52 Scan tasks



Scan Tasks

Task data from the last 30 days is automatically retained. Scan results are displayed on the Virus Scan page.

Unlimited | Pay-per-use

Enter a task name.

Task Name	Scan M...	Startup Type	Started	Associate...	Handling P...	Status	Result	Operation
Quick Scan-20...	Quick S...	Scan Now	Jun 19, 2025 19:3...	1	Manual Ha...	Scanning 0/1	0 | 0 | 0	Cancel
[redacted]	Custom...	Scan Now	Jun 19, 2025 17:1...	1	Manual Ha...	Complete	1 | 0 | 0	
[redacted]	Custom...	Periodic Start	Jun 19, 2025 17:0...	12	Manual Ha...	Complete	6 | 6 | 0	Scan Again
[redacted]	Custom...	Scan Now	Jun 19, 2025 16:4...	1	Manual Ha...	Complete	1 | 0 | 0	
[redacted]	Full-dis...	Scan Now	Jun 19, 2025 16:3...	1	Manual Ha...	Complete	0 | 0 | 1	Scan Again
[redacted]	Full-dis...	Scan Now	Jun 19, 2025 11:1...	1	Manual Ha...	Complete	1 | 0 | 0	
[redacted]	Custom...	Scan Now	Jun 19, 2025 11:0...	1	Automatic ...	Complete	1 | 0 | 0	

Step 3 Click ⌄ to view the scan status and number of scanned files of each server.

- Click **Cancel** in the **Operation** column of the server to stop scanning the server.
- To retry a failed scan on a server, click **Scan Again** in the **Operation** column of the server.

----End

Follow-up Operations

After a virus scan task is complete, you can manually handle the detected virus-infected files based on service requirements. For details, see **Viewing and Handling Viruses**.

6.6.3 Viewing and Handling Viruses

Scenarios

After the virus scanning is complete, HSS handles the virus-infected files based on the handling policy selected. The handling policies are as follows:

- Automatic handling: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled.
- Manual handling: Alarms are generated for the detected virus-infected files. You need to manually confirm the files before handling them.

No matter which handling policy you choose, you need to confirm and handle the scan results in a timely manner to protect your servers from viruses.

The section describes how to check and manually handle virus-infected files.

Prerequisites

A virus scanning task has been executed. For details, see **Scanning for Viruses**.

Viewing and Handling Viruses

Step 1 Log in to the management console.

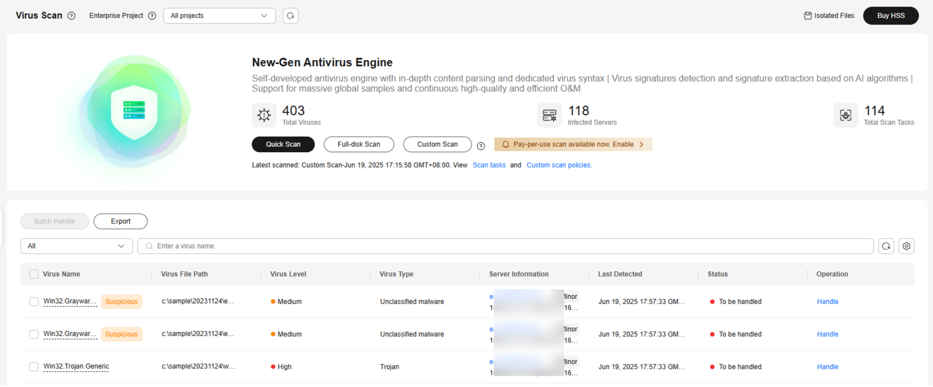
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 Choose **Server Protection** > **Virus Scan**.

Step 4 View the scanned virus files.

Hover the cursor over a virus name to view its file path, file hash, owner, attribute, size, and creation time.

Figure 6-53 Virus-infected file list



New-Gen Antivirus Engine

Self-developed antivirus engine with in-depth content parsing and dedicated virus syntax | Virus signatures detection and signature extraction based on AI algorithms | Support for massive global samples and continuous high-quality and efficient O&M

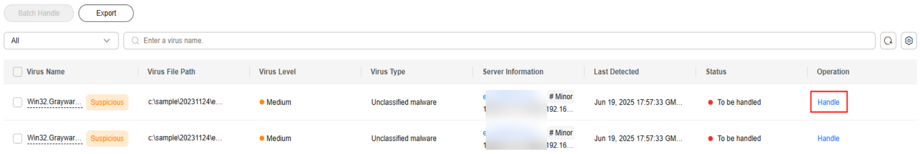
Latest scanned: Custom Scan-Jun 19, 2025 17:15:58 GMT+08:00. View Scan tasks and Custom scan policies.

Virus Name	Virus File Path	Virus Level	Virus Type	Server Information	Last Detected	Status	Operation
Win32.Graywar... Suspicious	c:\sample\20231124\e...	● Medium	Unclassified malware	[redacted]	Jun 19, 2025 17:57:33 GM...	● To be handled	Handle
Win32.Graywar... Suspicious	c:\sample\20231124\e...	● Medium	Unclassified malware	[redacted]	Jun 19, 2025 17:57:33 GM...	● To be handled	Handle
Win32.Trojan.Generic	c:\sample\20231124\w...	● High	Trojan	[redacted]	Jun 19, 2025 17:57:33 GM...	● To be handled	Handle

Step 5 In the **Operation** column of a virus file, click **Handle**.

You can also select multiple virus files and click **Batch Handle** above the list to handle them in batches.

Figure 6-54 Handling virus-infected files



Virus Name	Virus File Path	Virus Level	Virus Type	Server Information	Last Detected	Status	Operation
Win32.Graywar... Suspicious	c:\sample\20231124\e...	● Medium	Unclassified malware	[redacted]	Jun 19, 2025 17:57:33 GM...	● To be handled	Handle
Win32.Graywar... Suspicious	c:\sample\20231124\e...	● Medium	Unclassified malware	[redacted]	Jun 19, 2025 17:57:33 GM...	● To be handled	Handle

Step 6 In the **Handle Infected Files** dialog box, select a virus-infected file handling method. For more information, see **Virus-infected file handling methods**.

Table 6-41 Virus-infected file handling methods

Parameter	Description
Mark as handled	Select this if you have manually handled the virus-infected file on the server.
Ignore	Ignore the virus-infected file alarm. If this file is detected again, HSS generates an alarm.

Parameter	Description
Add to alarm whitelist	If you confirm that the virus file is falsely reported, you can add it to the alarm whitelist. After a file is added to whitelist, HSS will not generate alarms for the file.
Isolating files manually	Isolate virus-infected files. After a file is isolated, it will become read-only. To avoid impact on services, exercise caution when performing this operation. Isolated files are added to the **Isolated Files** and cannot harm your server. You can restore or delete isolated files as required. For details, see **Isolated Files**.

Step 7 Click **OK**.

After the alarm is handled, the status of the virus file alarm event changes to **Handled**. You can view the handling records on the historical handling records page. For details, see **Handling History**.

----End

Exporting Virus Alarms

Export virus alarms to a local PC.

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

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

Step 3 Choose **Server Protection** > **Virus Scan**.

Step 4 Above the virus-infected file alarm event list, click **Export** to export all virus-infected file alarm events to the local PC.

Step 5 View the export status in the upper part of the virus scan page. After the export is successful, obtain the exported information from the default file download address on the local host.

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

6.6.4 Managing Custom Antivirus Policies

Scenarios

A custom antivirus policy is generated for each custom antivirus task that starts periodically or at a specified time point. You can modify or delete such policies as needed.

The policy of a task scheduled to be executed at a specified time point will expire after execution, and will be marked with an expiration tag. You can change the startup time of the policy and enable it again.

Editing a Custom Scan Policy

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Virus Scan**.

Step 4 Choose **Custom scan policies** to view existing user-defined antivirus policies.

Step 5 In the **Operation** column of a policy, click **Edit**. Modify the policy on the edit page. For more information, see Table 6-42.

Table 6-42 Custom antivirus policy parameters

Parameter	Description	Example Value
Task Name	HSS automatically generates a task name based on the task creation time (accurate to seconds). You can modify it as needed.	Custom Scan-20250425180036
Startup Type	Scan task execution type. ● **Scan Now**: Start a scan immediately. ● **Scan Later**: Start a scan at the specified time. ● **Periodic Start**: Start a scan periodically based on your settings.	Scan Later
Start	If **Startup Type** is set to **Scan Later**, configure this parameter to set the start time of the scan. You can set the start time to a time within one month.	2025/04/25 18:10
Schedule	If **Startup Type** is set to **Periodic Start**, configure this parameter to set the scan period.	-
File Type	Type of the file to be scanned. Currently, the following types of files can be scanned: ● **Executable**: executable files and dynamic link libraries (DLLs), such as .exe, .dll, and .so files ● **Compressed**: installation packages or other compressed packages, such as .zip, .rar, and .tar files ● **Script**: script files, such as .bat, .py, and .ps1 files ● **Document**: document files, such as .txt, .doc, and .pdf files ● **Image**: image files, such as .bmp, .jpg, and .gif files ● **Audio & Video**: audiovisual files, such as .mp3, .mp4, and .flv files	Select All

Parameter	Description	Example Value
(Optional) Directory Settings	Directory where virus-infected files need to be scanned. If this parameter is not set, full scan is performed by default. Full scan does not cover network directories.	-
(Optional) Exclude Specified Directories	Directories that do not require virus scan.	-
Select Server	Select the servers to be scanned. You can select and scan servers that meet all the following conditions: ● The agent is online and meets the following requirements: For details about how to install the agent, see **Installing the Agent on Servers**. – Unlimited scans: Windows agent version ≥ 4.0.20, Linux agent version ≥ 3.2.9 – Pay-per-use scans: Windows agent version ≥ 4.0.23, Linux agent version ≥ 3.2.12 ● The AV detection policy is enabled. For details about how to enable it, see **Configuring Policies**. ● The task start conditions required by the corresponding policy are met: – Policy whose **Startup Type** is **Scan Now**: The server is not being scanned. – Policy whose **Startup Type** is **Scan Later**: No other custom scan policies using the same startup time as the current policy are bound to the server. – Policy whose **Startup Type** is **Periodic Start**: No other custom policies whose **Startup Type** is **Periodic Start** are bound to the server.	-

Parameter	Description	Example Value
Handling Policy	Action to be taken on the detected virus-infected files. ● **Automatic Handling**: HSS automatically isolates the detected malicious files. The suspicious files that are not confirmed as viruses are labeled as suspicious and need to be manually checked and handled. **CAUTION** In rare cases, files may be incorrectly isolated. In this case, you can restore the isolated files on the **Isolated Files** page. For details, see **Restoring Isolated Files**. ● **Manual Handling**: Alarms are generated only for detected infected files. You need to manually confirm the files before handling them.	Automatic Handling

Step 6 Click **OK**.

----End

Deleting a Custom Scan Policy

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

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

Step 3 Choose **Server Protection** > **Virus Scan**.

Step 4 Choose **Custom scan policies** to view existing user-defined antivirus policies.

Step 5 Click **Delete** in the **Operation** column of a policy.

To delete policies in batches, you can also select multiple policies and click **Delete** in the upper left corner of the list.

Step 6 Click **OK**.

----End

6.6.5 Managing Isolated Files

Scenarios

Isolated files are added to the **Isolated Files** and cannot harm your server. You can also refer to this section to restore or delete isolated files as required.

- **Restoring Isolated Files**: If an isolated file is a normal service file and not infected by any viruses, you can restore the file.

- **Deleting Isolated Files**: If an isolated file is infected by a virus, delete the file to completely remove the virus.

Restoring Isolated Files

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Virus Scan**.

Step 4 Click **Isolated Files** in the upper right corner of the page. The dialog box is displayed.

Step 5 Click **Restore** in the **Operation** column of the list. The dialog box is displayed.

Step 6 Click **OK**.

If the file can be used after being restored, the restoration is successful.

----End

Deleting Isolated Files

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Virus Scan**.

Step 4 Click **Isolated Files** in the upper right corner of the page. The dialog box is displayed.

Step 5 Click **Delete** in the **Operation** column of the list. The dialog box is displayed.

To delete isolated files in batches, select multiple isolated files and click **Delete** in the upper left corner of the list.

Step 6 Click **OK**.

If the file cannot be found on the **Isolated Files** page, deletion is successful.

----End

6.7 Dynamic Port Honeypot

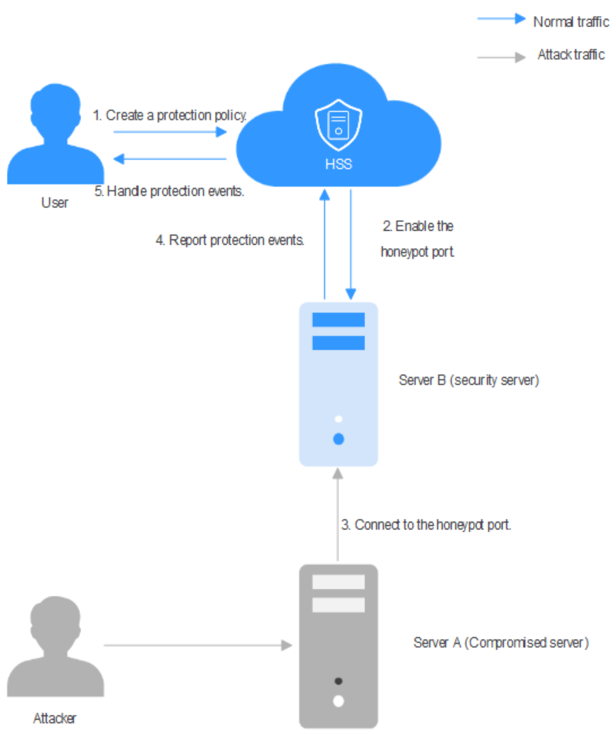
6.7.1 Dynamic Port Honeypot Overview

What is Dynamic Port Honeypot?

The dynamic port honeypot function is a deception trap. It uses a real port as a honeypot 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 real resources of the user.

You can enable the dynamic port honeypot using recommended ports or user-defined ports to deceive compromised servers and reduce the risk of resources intrusion. Figure 6-55 shows how the dynamic port honeypot works.

Figure 6-55 Dynamic port honeypot protection


Normal traffic
Attack traffic
User
1. Create a protection policy.
5. Handle protection events.
HSS
4. Report protection events.
2. Enable the honeypot port
Server B (security server)
3. Connect to the honeypot port.
Attacker
Server A (Compromised server)

How Do I Use Dynamic Port Honeypot?

Figure 6-56 shows the process of using the dynamic port honeypot.

Figure 6-56 Process of using the dynamic port honeypot

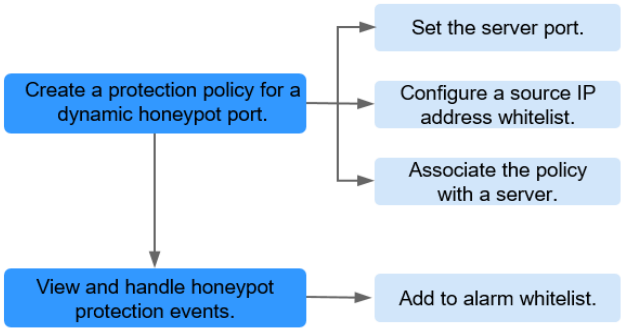

Create a protection policy for a dynamic honeypot port.
Set the server port.
Configure a source IP address whitelist.
Associate the policy with a server.
View and handle honeypot protection events.
Add to alarm whitelist.

Table 6-43 Process of using the dynamic port honeypot

Operation	Description
Creating a Protection Policy for a Dynamic Honeypot Port	Enable the server port of dynamic port function, configure the source IP address whitelist, and bind the protected server.
Viewing and Handling Honeypot Protection Events	The dynamic port honeypot function reports an alarm when a potentially compromised server proactively connects to a honeypot port. You can handle the alarm based on service requirements.

Constraints

- Dynamic port honeypots apply only to servers that are not bound to EIPs.
- Dynamic port honeypots are available only in HSS premium, web tamper protection, and container editions. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.
- To use the dynamic port honeypots, ensure that the agent installed on the server falls within the following ranges. For more information, see **Upgrading the Agent**.
  - Linux: 3.2.10 or later.
  - Windows: 4.0.22 or later.

6.7.2 Creating a Protection Policy for a Dynamic Honeypot Port

Scenario

The dynamic port honeypot function uses a real port as a honeypot port to induce attackers to access the network. Therefore, when enabling dynamic port honeypot protection, you need to create a protection policy to add a server port as a honeypot port and bind it to the server for protection.

This chapter describes how to create a dynamic port honeypot protection policy.

Constraints

- A maximum of 10 honeypot ports can be added to a server.
- A honeypot port can be bound to only one protocol. Both TCP and TCP6 are supported.

Creating a Protection Policy for a Dynamic Honeypot Port

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 On the **Servers** tab, click **Create a Protection Policy**. The dialog box is displayed.

Step 6 Create a protection policy as prompted.

1. Configure the policy and click **Next**. For details about related parameters, see Table 6-44

Table 6-44 Parameters for creating a protection policy

Parameter	Description
Policy Name	You can retain the default name or enter a name that is easy to identify.
OS Type	Select an OS type of a server to which you want to add the dynamic port honeypot function.
Protected Port	Select a server port that implements the dynamic port honeypot function. – **Recommended Port**: For Linux, common Windows ports are recommended. For Windows, common Linux ports are recommended. – **Custom Port**: You can add custom ports or delete some recommended ports as required. **NOTE** Ensure that the port to be added is not occupied by other services. If the port is occupied, the dynamic port honeypot function fails to be enabled.
(Optional) Source IP address whitelist	By default, the servers that proactively connect to the dynamic honeypot port are compromised intranet servers. Once a suspicious connection behavior is detected, an alarm is reported. Therefore, if a trusted server may connect to the port, you are advised to add the IP address to the source IP address whitelist.

2. Select the target server and click **Save and Enable**.

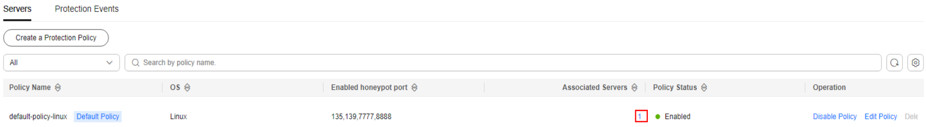
   Note that the dynamic port honeypot can be selected only for the servers that meet all the following conditions:

   – The HSS premium edition or higher has been enabled on the server.

- The server agent is online. The Windows agent version is 4.0.22 or later, and the Linux agent version is 3.2.10 or later.
- No dynamic port honeypot policies have been bound to the server.
- The OS type of the server is the same as that specified in **Step 6.1**.
- No EIPs have been bound to the server.

Step 7 In the **Associated Servers** column of the created target policy, click the value. The dialog box is displayed.

Figure 6-57 Associate servers



Policy Name	OS	Enabled honeypot port	Associated Servers	Policy Status	Operation
default-policy-linux Default Policy	Linux	135,139,7777,8888	1	● Enabled	Disable Policy Edit Policy Dele

Step 8 In the **Port Status** column of the associated server, check the port status.

To enable the port again, click the **Edit Policy** to select server, and then bind the server. For details about how to edit a policy, see **Editing a Policy**.

----End

FAQs

What can I do if the port fails to be enabled?

- Possible cause 1: The port is occupied by other services.

  Solution: Add other idle ports by editing the policy.

- Possible cause 2: System resources are insufficient.

  Solution: Free up some system resources, click the **Edit Policy** to select server, and then bind the server. For details about how to edit a policy, see **Editing a Policy**.

6.7.3 Viewing and Handling Honeypot Protection Events

Scenario

By default, the servers that proactively connect to the dynamic honeypot port are compromised intranet servers. Once a suspicious connection behavior is detected, an alarm is reported.

This chapter describes how to view and handle these alarms and events.

Viewing and Handling Honeypot Protection Events

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

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

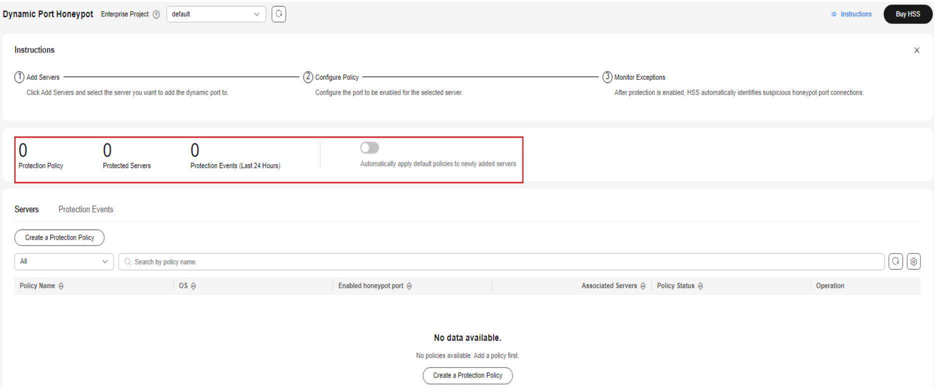
Step 3 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Under the introductions, view the protection overview.

- You can view the number of protection policies, protected servers, and protection events.
- You can enable the **Automatically apply default policies to newly add servers**. If is displayed, the function is enabled.

Figure 6-58 Protection overview



Instructions

1. Add Servers: Click Add Servers and select the server you want to add the dynamic port to.
2. Configure Policy: Configure the port to be enabled for the selected server.
3. Monitor Exceptions: After protection is enabled, HSS automatically identifies suspicious honeypot port connections.

0 Protection Policy
0 Protected Servers
0 Protection Events (Last 24 Hours)

Automatically apply default policies to newly added servers

Policy Name	OS	Enabled honeypot port	Associated Servers	Policy Status	Operation

No data available.

No policies available. Add a policy first.

Step 6 Click the **Protection Events** tab to view honeypot protection events. For details about the parameters in the event list, see **Table 6-45**.

Table 6-45 Parameters in the event list

Parameter	Description
Alarm Name	The name of an alarm event. Click an alarm name to view the details. For details, see **Table 6-47**.
Alert Severity	Alarm threat level. Honeypot protection events are classified into the following two levels: ● High risk: The remote server connects to the honeypot port for multiple times. ● Medium risk: The remote server is connected to the honeypot port.
Alarm Summary	Summary of alarm events. Based on the information, you can learn about the server that may be compromised and the connection between the server and the port.
Affected Asset	Dynamic port server connected to the compromised server.
Alarm Reported	Time when an alarm occurred.
Status	Alarm handling status, which can be **Handled** or **To be handled**.
Operation	You can handle alarm events.

Step 7 After confirming the alarm information, click **Handle** in the **Operation** column of the event whose **Status** is **To be handled**. The **Handle Alarm** dialog box is displayed.

If you need to handle multiple alarm events in batches, click **Batch Handle** in the upper left corner of the list.

Step 8 Select a solution. For details about the solution, see **Table 6-46**.

Table 6-46 Parameters for handling alarm events

Parameter	Description
Action	● **Ignore**: Ignore the alarm event. The alarm is still generated when the next threat event occurs. ● **Mark as handled**: You have manually isolated ports for the compromised server. ● **Add to alarm whitelist**: Add the trusted server that triggers an alarm to the whitelist so that no alarm will be generated when similar events occur.
Batch Handle	If you need to handle the same alarm event at the same time, you can select the parameter.
(Optional) Remarks	To facilitate identification of the current processing, supplementary description can be provided.

Step 9 Click **OK**.

----End

Alarm Details Parameters

For details about the parameters on the alarm details, see **Table 6-47**.

Table 6-47 Alarm details parameters

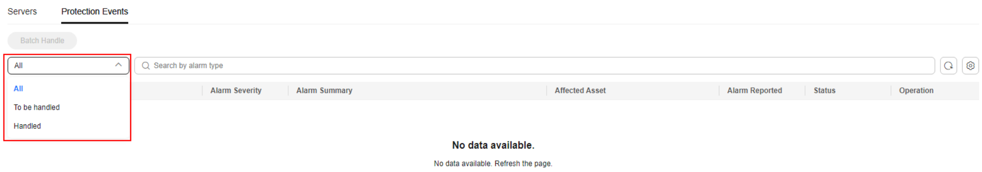
Parameter	Description
Intelligence Engine	Detection engines used by HSS, including the virus detection engine, AI detection engine, and malicious intelligence detection engine.
Attack Status	Status of the current threat.
First Occurred	Time when an attack alarm is generated for the first time
Alarm ID	Unique ID of an alarm

Parameter	Description
ATT&CK Phase	Attack model used by attackers in each phase.
Last Occurred	Time when an attack alarm was last generated
Alarm Information	Detailed information about an alarm, including the alarm description, alarm summary, affected assets, and handling suggestions.
Forensics	The dynamic port honeypot function checks the network forensics information of the attack source.
Similar Alarms	Alarms that are similar to the current alarm event. You can handle the alarm according to the handling method of the similar alarms.

Filtering Events in Different Handling Statuses

Select an event in the target status from the drop-down list.

Figure 6-59 Filtering events



No data available.

No data available. Refresh the page.

6.7.4 Managing Dynamic Port Honeypot Protection Policies

Scenario

After a policy is created, you can manage the policy based on your protection requirements.

- **Disabling a policy**: Disable the dynamic port honeypot function temporarily.
- **Enabling a policy**: Enable a disabled function of dynamic port honeypot.
- **Editing a policy**: Modify the protection policy information of dynamic port honeypot, for example, adding or deleting ports, and unbinding or binding servers.
- **Deleting a policy**: Delete the dynamic port honeypot protection policy and disable the function.

Constraints

The default policy cannot be deleted.

Disabling a Policy

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the row containing the target policy, click **Disable Policy** in the **Operation** column. The dialog box is displayed.

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

----End

Enabling a Policy

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the row containing the target policy, click **Enable Policy** in the **Operation** column. The dialog box is displayed.

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

----End

Editing a Policy

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the row containing the target policy, click **Edit Policy** in the **Operation** column. The dialog box is displayed.

Step 6 Configure a policy.

You can modify the policy name, protected port, and source IP address whitelist.

Step 7 Click **Next**.

Step 8 Select a server to be bound.

Step 9 Click **OK**.

----End

Delete a Policy

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

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

Step 3 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the row containing the target policy, click **Delete** in the **Operation** column. The **Delete Policy** dialog box is displayed.

Step 6 Ensure that all information is correct and click **OK**.

----End

6.7.5 Managing Associated Servers

Scenario

For servers associated with a protection policy, you can **switch the protection policy** for servers or **unbind the protection policy** from the servers.

Changing a Policy

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

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

Step 3 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the **Associated Servers** column of the target policy, click the value. The dialog box is displayed.

Step 6 Click **Change Policy** in the **Operation** column. The **Change Policy** dialog box is displayed.

To switch protection policies for multiple servers, select all target servers and click **Change Policy** in the upper left corner of the list.

Step 7 Select a protection policy as prompted.

Step 8 Click **OK**.

----End

Unbinding a Policy

Step 1 Log in to the management console.

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

Step 3 Choose **Server Protection** > **Dynamic Port Honeypot**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 In the **Associated Servers** column of the target policy, click the value. The dialog box is displayed.

Step 6 Click **Unbind** in the **Operation** column. The **Unbind** dialog box is displayed.

To unbind multiple servers, select all target servers and click **Unbind** in the upper left corner of the list.

Step 7 Confirm the information and click **OK**.

----End

7 Container Protection

7.1 Container Firewalls

7.1.1 Container Firewall Overview

A container firewall controls and intercepts network traffic inside and outside a container cluster to prevent malicious access and attacks.

Constraints

- The container firewall is available only in the HSS container edition. For details about how to purchase HSS, see **Purchasing an HSS Quota**.
- The following container network models can be protected:
  - CCE clusters: container tunnel network model, cloud native network 2.0 model, and VPC network model
  - Other Kubernetes clusters: Only the built-in network policy of Kubernetes (the native Kubernetes network) is supported.
- In a CCE cluster, to operate resource objects, you need to obtain either of the following operation permissions:
  - IAM permissions: Tenant Administrator or CCE Administrator.
  - Namespace permissions (authorized by Kubernetes RBAC): O&M permissions. For details about how to configure permissions, see **Configuring namespace permissions**.

How It Works

A container firewall controls the access scope of source and destination containers based on the access policies for pods and servers, blocking internal and external malicious accesses and attacks.

Related Operations

- **Configuring a Network Defense Policy (for a Container Tunnel Network)**

- Configuring a Network Defense Policy (for a VPC Network)
- Configuring a Network Defense Policy (for Cloud Native Network 2.0)
- Configuring a Network Defense Policy (for a Native Kubernetes Network)

7.1.2 Configuring a Network Defense Policy (for a Container Tunnel Network)

You can configure network defense policies to limit the access traffic to the pods in a cluster using the container tunnel network model. If no network policies are configured, all the inbound and outbound traffic of the pods in a namespace are allowed by default.

This section describes how to configure a network policy for a cluster using the container tunnel network model.

Constraints

- Network policies have the following constraints:
  - Inbound rules, which are supported by all cluster versions.
  - Outbound rules, which are supported only by clusters in version 1.23 and later.
- Network isolation is not supported for IPv6 addresses.

Creating a Network Defense Policy

You can create a network defense policy in various ways.

Creating a Network Policy from YAML

Step 1 Log in to the management console.

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

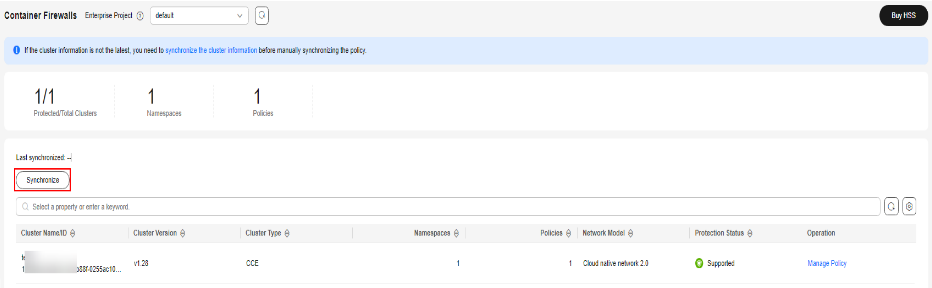
Step 3 In the navigation pane on the left, choose **Container Protection** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on clusters.

The synchronization takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Figure 7-1 Synchronizing CCE cluster policies



Container Firewalls Enterprise Project default Buy HSS

If the cluster information is not the latest, you need to synchronize the cluster information before manually synchronizing the policy.

1/1 Protected/Total Clusters

1 Namespaces

1 Policies

Last synchronized: --

Synchronize

Select a property or enter a keyword.

Cluster Name/ID	Cluster Version	Cluster Type	Namespaces	Policies	Network Model	Protection Status	Operation
[redacted] b88f-0255ac10...	v1.28	CCE	1	1	Cloud native network 2.0	Supported	Manage Policy

Step 6 Click **Manage Policy** in the **Operation** column of a cluster using the container tunnel network model.

Step 7 Click **Create from YAML** above the policy list.

Step 8 On the YAML creation page, enter content or click **Import**.

The following is an example of a network policy created using YAML. The network policy requires that a pod can only be accessed by pods with specific labels and can only access specific pods.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: access-demo4
  namespace: default
spec:
  policyTypes:
  - Ingress
  - Egress
  podSelector:                    # The rule takes effect for pods with the role=db label.
    matchLabels:
      role: db
  ingress:                       # Ingress rule
  - from:
    - podSelector:                # Only allow the access of the pods labeled with role=frontend.
        matchLabels:
          role: frontend
    ports:                       # Only TCP can be used to access port 6379.
    - protocol: TCP
      port: 6379
  egress:                        # Egress rule
  - to:
    - podSelector:                # Only pods with the role=web label can be accessed.
        matchLabels:
          role: web
```

Step 9 Click **OK**.

You can view the new policy in the policy management list.

----End

Creating a Network Policy on the GUI

Step 1 Log in to the management console.

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

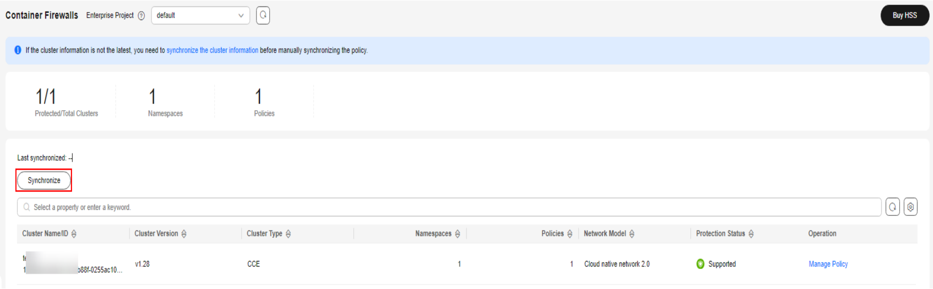
Step 3 In the navigation pane on the left, choose **Container Protection** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on clusters.

The synchronization takes about 1 to 2 minutes. Wait for a while and click ↻ in the upper right corner of the list to refresh and view the latest data.

Figure 7-2 Synchronizing CCE cluster policies



If the cluster information is not the latest, you need to synchronize the cluster information before manually synchronizing the policy.

Cluster Name/ID	Cluster Version	Cluster Type	Namespaces	Policies	Network Model	Protection Status	Operation
[redacted] b88f-0255ac10...	v1.28	CCE	1	1	Cloud native network 2.0	Supported	Manage Policy

Step 6 Click **Manage Policy** in the **Operation** column of a cluster using the container tunnel network model.

Step 7 Click **Create Network Policy** above the network policy list.

- **Policy Name**: Enter a network policy name.
- **Namespace**: Select the namespace of the network policy.
- **Selector**: Enter a key and a value to set the pod to be associated, and click **Add**. You can also click **Reference Workload Label** to reference the label of an existing workload.
- Inbound rule: Click **Add Rule** in the **Inbound Rules** area. For more information, see **Table 7-1**.

Table 7-1 Adding an inbound rule

Parameter	Description
Protocol & Port	Enter the inbound protocol type and port number of the pods to be associated. Currently, TCP and UDP are supported. If this parameter is not specified, all access traffic is allowed.
Source Namespace	Select a namespace whose objects can be accessed. If this parameter is not specified, access to the objects that belong to the same namespace as the current policy is allowed.
Source Pod Label	Select a label. Pods with this label can be accessed. If this parameter is not specified, all pods in the namespace can be accessed.

- Outbound rule: Click **Add Rule** in the **Outbound Rules** area. For more information, see **Table 7-2**.

Table 7-2 Adding an outbound rule

Parameter	Description
Protocol & Port	Enter the port and protocol of destination objects. If this parameter is not specified, access is not limited.
Destination CIDR Block	Configure CIDR blocks. This parameter allows requests to be routed to a specified CIDR block (and not to the exception CIDR blocks). Separate the destination and exception CIDR blocks by vertical bars (|), and separate multiple exception CIDR blocks by commas (,). For example, 172.17.0.0/16|172.17.1.0/24,172.17.2.0/24 indicates that 172.17.0.0/16 is accessible, but not for 172.17.1.0/24 or 172.17.2.0/24.
Destination Namespace	Namespace where the destination object is located. If not specified, the object belongs to the same namespace as the current policy.
Destination Pod Label	Select a label. Pods with this label can be accessed. If this parameter is not specified, all pods in the namespace can be accessed.

Step 8 Click **OK**.

You can view the new policy in the policy management list.

----End

Related Operations

Modifying or deleting a network policy

Step 1 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 2 Click **Manage Policy** in the **Operation** column of a cluster using the container tunnel network model.

Step 3 Click **Synchronize** above the network policy list.

The synchronization takes about 1 to 2 minutes. Wait for a while and click ↻ in the upper right corner of the list to refresh and view the latest data.

Step 4 Manage policies as needed.

- Modifying a policy
  - In the **Operation** column of a policy, click **Edit YAML**. On the YAML page, modify the YAML content and click **OK**.
  - In the **Operation** column of a policy, click **Update**. Modify the network policy information and click **OK**.
- Deleting a policy

- In the **Operation** column of a policy, click **Delete**. In the confirmation dialog box, click **OK**.
- Select one or multiple policies and click **Delete** above the policy list. In the displayed dialog box, click **OK**.

----End

7.1.3 Configuring a Network Defense Policy (for a VPC Network)

For clusters using the VPC network model, you can configure network defense policies to limit the traffic that accesses the servers where containers are deployed. If no security group rules are configured, all incoming and outgoing traffic of the servers is allowed by default.

This section describes how to configure a network defense policy for a cluster using the VPC network model.

Creating a Network Defense Policy

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Container Protection** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on clusters.

The synchronization takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Step 6 Click **Manage Policy** in the **Operation** column of a cluster using the VPC network model.

Step 7 In the **Operation** column of a node, click **Configure Policy**.

Step 8 In the displayed dialog box, click **OK** to go to the cloud server console.

Step 9 Click the **Security Groups** tab and view security group rules.

Step 10 Click **Manage Rule**. The security group page is displayed.

Step 11 Configure inbound and outbound rules.

For details, see **Adding a Security Group Rule**.

----End

Related Operations

Modifying or deleting a network defense policy

Step 1 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 2 Click **Manage Policy** in the **Operation** column of a cluster using the VPC network model.

Step 3 Click **Synchronize** above the node list to synchronize node information.

The synchronization takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Step 4 In the **Operation** column of a node, click **Configure Policy**.

Step 5 In the displayed dialog box, click **OK** to go to the cloud server console.

Step 6 Click the **Security Groups** tab and view security group rules.

Step 7 Click **Manage Rule**. The security group page is displayed.

Step 8 Click a rule tab and manage rules as needed.

- Modifying a rule

  In the **Operation** column of a rule, click **Modify**. Modify the rule and click **OK**.

- Deleting a rule

  In the **Operation** column of a rule, click **Delete**. In the confirmation dialog box, click **OK**.

----End

7.1.4 Configuring a Network Defense Policy (for Cloud Native Network 2.0)

For clusters using the cloud native network 2.0 model, you can configure network defense policies to limit the traffic that accesses the servers where containers are deployed. If no security group policies are configured, all incoming and outgoing traffic of the servers is allowed by default.

This chapter describes how to create a network defense policy for a cluster using the cloud native network 2.0 model.

Creating a Network Defense Policy

Step 1 Log in to the management console.

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

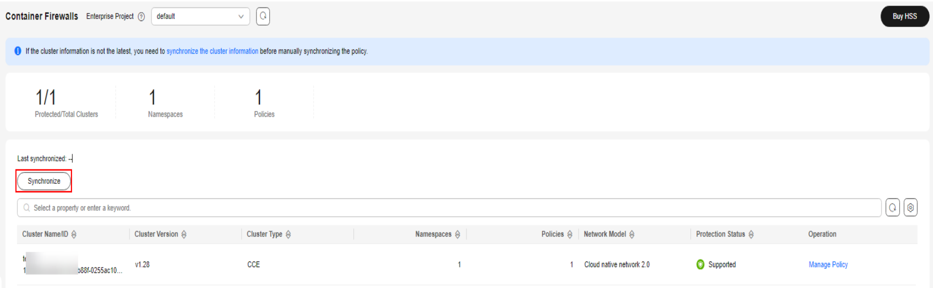
Step 3 In the navigation pane on the left, choose **Container Protection** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on clusters.

The synchronization takes about 1 to 2 minutes. Wait for a while and click 🔄 in the upper right corner of the list to refresh and view the latest data.

Figure 7-3 Synchronizing CCE cluster policies



Container Firewalls Enterprise Project ⓘ default

Buy HSS

If the cluster information is not the latest, you need to synchronize the cluster information before manually synchronizing the policy.

1/1 Protected/Total Clusters | 1 Namespaces | 1 Policies

Last synchronized: --

Synchronize

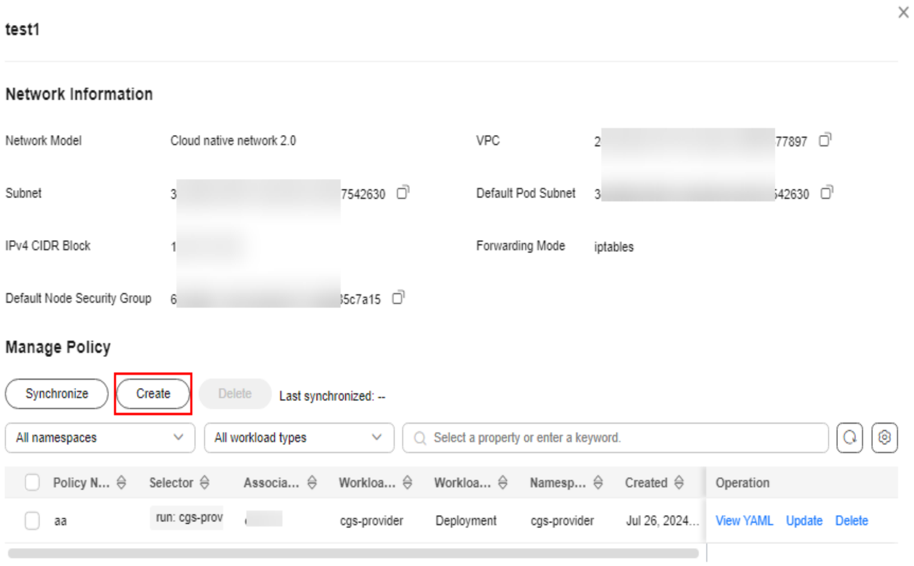
Select a property or enter a keyword.

Cluster Name/ID	Cluster Version	Cluster Type	Namespaces	Policies	Network Model	Protection Status	Operation
te 1 b88f-0255ac10...	v1.28	CCE	1	1	Cloud native network 2.0	Supported	Manage Policy

Step 6 Click **Manage Policy** in the **Operation** column of a cluster using the cloud native network 2.0 model.

Step 7 Click **Create** above the policy list. The **Create a Security Group Policy** dialog box is displayed.

Figure 7-4 Policy management



test1

Network Information

Network Model	Cloud native network 2.0	VPC	2 77897
Subnet	3 7542630	Default Pod Subnet	3 542630
IPv4 CIDR Block	1	Forwarding Mode	iptables
Default Node Security Group	6 5c7a15		

Manage Policy

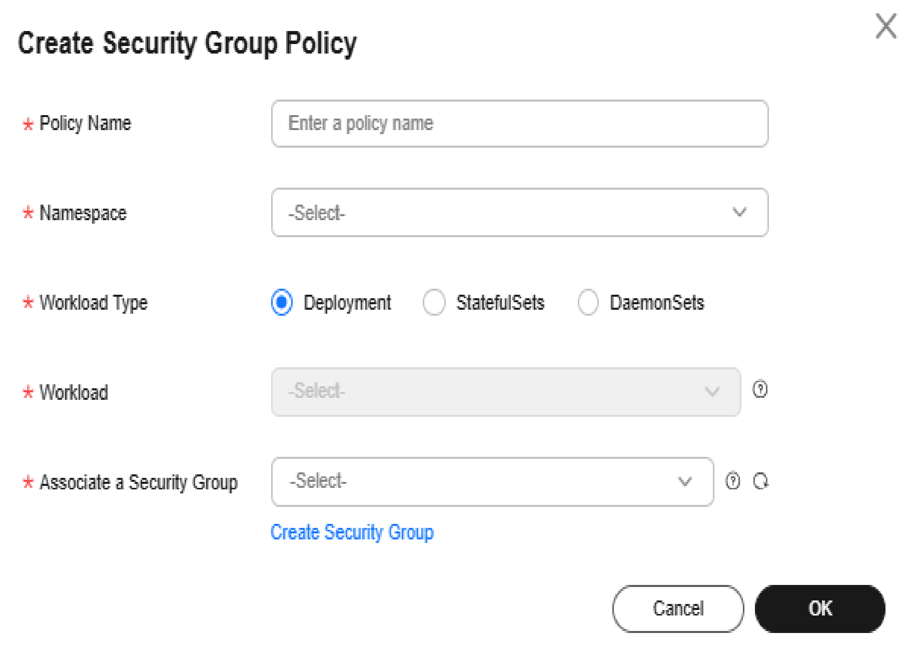
Synchronize Create Delete Last synchronized: --

All namespaces | All workload types | Select a property or enter a keyword.

□	Policy N...	Selector	Associa...	Workloa...	Workloa...	Namesp...	Created	Operation
□	aa	run: cgs-prov		cgs-provider	Deployment	cgs-provider	Jul 26, 2024...	View YAML Update Delete

Step 8 Enter the policy information as prompted. For details about related parameters, see **Table 7-3**.

Figure 7-5 Create a security group policy



Create Security Group Policy

*Policy Name: Enter a policy name

*Namespace: -Select-

*Workload Type: ● Deployment ○ StatefulSets ○ DaemonSets

*Workload: -Select-

*Associate a Security Group: -Select-

Table 7-3 Parameters for creating a security group policy

Parameter	Description
Policy	Enter a policy name.
Namespace	A namespace to be selected.
Workload Type	Select a load type. The following types are supported: ● Deployment ● StatefulSets ● DaemonSets
Workload	Select the target workload.
Associate a Security Group	Select a security group to be associated. Each policy can be associated with a maximum of five groups. The existing security groups in the list are those you have created in the VPC service. To create a security group, click **Create a Security Group** to go to the VPC console. For details, see **Create a Security Group**.

Step 9 After entering the policy information, click **OK**.

You can view the new policy in the policy management list.

----End

Related Operations

Modifying or deleting a network defense policy

Step 1 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

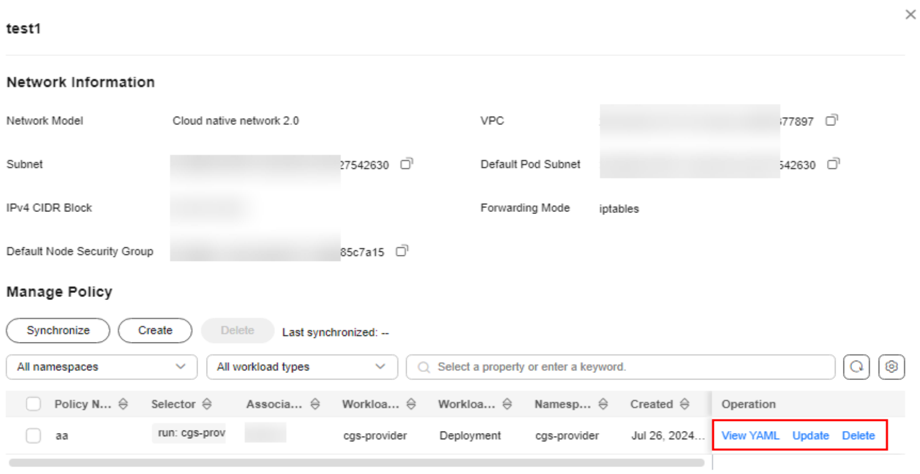
Step 2 Click **Manage Policy** in the **Operation** column of a cluster using the cloud native network 2.0 model.

Step 3 Click **Synchronize** above the policy list to synchronize cluster policy information.

The synchronization takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Step 4 Select the operation to be performed on the policy.

Figure 7-6 Managing policies



test1

Network Information

Network Model	Cloud native network 2.0	VPC	[redacted]77897
Subnet	[redacted]27542630	Default Pod Subnet	[redacted]542630
IPv4 CIDR Block	[redacted]	Forwarding Mode	iptables
Default Node Security Group	[redacted]85c7a15		

Manage Policy

Last synchronized: --

	Policy N...	Selector	Associa...	Workloa...	Workloa...	Namesp...	Created	Operation
□	aa	run: cgs-prov	[redacted]	cgs-provider	Deployment	cgs-provider	Jul 26, 2024...	View YAML Update Delete

- View policy content.

  In the **Operation** column of a policy, click **View YAML**. In the displayed dialog box, you can select **YAML** or **JSON** to view the policy details. Click **Download** in the upper left corner of the dialog box.

- Update policy content.

  a. Locate a target policy and click **Update** in the **Operation** column. The **Update a Security Group Policy** dialog box is displayed.

  b. Add or delete an associated security group.

  c. Click **OK**.

- Delete a policy.

  a. Locate a target policy and click **Delete** in the **Operation** column. The **Delete Policy** dialog box is displayed.

  b. Ensure that all information is correct and click **OK**.

----End

7.1.5 Configuring a Network Defense Policy (for a Native Kubernetes Network)

You can configure a network defense policy to restrict the traffic to the pods in a cluster that uses the built-in Kubernetes network policy. If no network policies are configured, all the inbound traffic of the pods in a namespace are allowed by default.

This section describes how to configure a network policy for a cluster using the native Kubernetes network model.

Constraints

Kubernetes 1.23 and later versions support inbound and outbound rules. Versions earlier than Kubernetes 1.23 support only inbound rules.

Creating a Network Defense Policy

You can create a network defense policy in various ways.

Creating a Network Policy from YAML

Step 1 Log in to the management console.

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

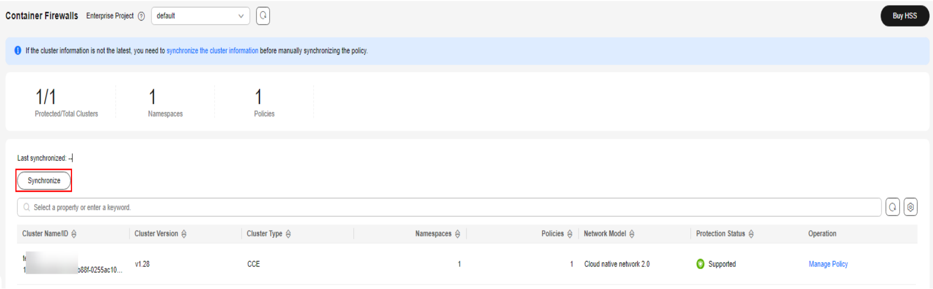
Step 3 In the navigation pane on the left, choose **Container Protection** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on clusters.

The synchronization takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Figure 7-7 Synchronizing CCE cluster policies



Container Firewalls Enterprise Project default

If the cluster information is not the latest, you need to synchronize the cluster information before manually synchronizing the policy.

1/1 Protected/Total Clusters
1 Namespaces
1 Policies

Last synchronized: --

Cluster Name/ID	Cluster Version	Cluster Type	Namespaces	Policies	Network Model	Protection Status	Operation
[redacted]b88f-0255ac10...	v1.28	CCE	1	1	Cloud native network 2.0	Supported	Manage Policy

Step 6 Click **Manage Policy** in the **Operation** column of the cluster using the native Kubernetes network model. The policy management page is displayed.

Step 7 Click **Create from YAML** above the policy list.

Step 8 On the YAML creation page, enter content or click **Import**.

The following is an example of a network policy created using YAML. The network policy allows pods to be accessed only by the pods with specific labels.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: access-demo1
  namespace: default
spec:
  podSelector:                  # The rule takes effect for pods with the role=db label.
    matchLabels:
      role: db
  ingress:                      # Ingress rule
  - from:
    - podSelector:              # Only allow the access of the pods labeled with role=frontend.
        matchLabels:
          role: frontend
    ports:                      # Only TCP can be used to access port 6379.
    - protocol: TCP
      port: 6379
```

Step 9 Click **OK**.

You can view the new policy in the policy management list.

----End

Creating a Network Policy on the GUI

Step 1 Log in to the management console.

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

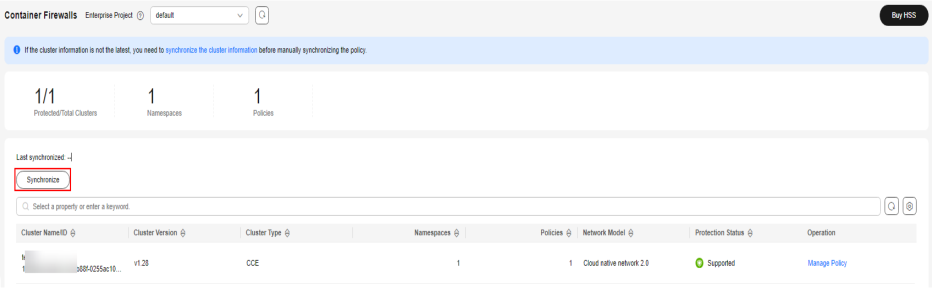
Step 3 In the navigation pane on the left, choose **Container Protection** > **Container Firewalls**.

Step 4 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 5 Click **Synchronize** above the cluster list to synchronize the policies created on clusters.

The synchronization takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Figure 7-8 Synchronizing CCE cluster policies



Container Firewalls Enterprise Project: default

If the cluster information is not the latest, you need to synchronize the cluster information before manually synchronizing the policy.

1/1 Protected/Total Clusters | 1 Namespaces | 1 Policies

Last synchronized: --

Select a property or enter a keyword.

Cluster Name/ID	Cluster Version	Cluster Type	Namespaces	Policies	Network Model	Protection Status	Operation
[redacted]b88f-0255ac10...	v1.28	CCE	1	1	Cloud native network 2.0	Supported	Manage Policy

Step 6 Click **Manage Policy** in the **Operation** column of the cluster using the native Kubernetes network model. The policy management page is displayed.

Step 7 Click **Create Network Policy** above the network policy list.

- **Policy Name**: Enter a network policy name.
- **Namespace**: Select the namespace of the network policy.
- **Selector**: Enter a key and a value to set the pod to be associated, and click **Add**. You can also click **Reference Workload Label** to reference the label of an existing workload.
- Inbound rule: Click **Add Rule** in the **Inbound Rules** area. For more information, see **Table 7-4**.

Table 7-4 Adding an inbound rule

Parameter	Description
Protocol & Port	Enter the inbound protocol type and port number of the pods to be associated. Currently, TCP and UDP are supported. If this parameter is not specified, all access traffic is allowed.
Source Namespace	Select a namespace whose objects can be accessed. If this parameter is not specified, access to the objects that belong to the same namespace as the current policy is allowed.
Source Pod Label	Select a label. Pods with this label can be accessed. If this parameter is not specified, all pods in the namespace can be accessed.

- Outbound rule: Click **Add Rule** in the **Outbound Rules** area. For more information, see **Table 7-5**.

Table 7-5 Adding an outbound rule

Parameter	Description
Protocol & Port	Enter the port and protocol of destination objects. If this parameter is not specified, access is not limited.
Destination CIDR Block	Configure CIDR blocks. This parameter allows requests to be routed to a specified CIDR block (and not to the exception CIDR blocks). Separate the destination and exception CIDR blocks by vertical bars (|), and separate multiple exception CIDR blocks by commas (,). For example, 172.17.0.0/16|172.17.1.0/24,172.17.2.0/24 indicates that 172.17.0.0/16 is accessible, but not for 172.17.1.0/24 or 172.17.2.0/24.

Parameter	Description
Destination Namespace	Namespace where the destination object is located. If not specified, the object belongs to the same namespace as the current policy.
Destination Pod Label	Select a label. Pods with this label can be accessed. If this parameter is not specified, all pods in the namespace can be accessed.

Step 8 Click **OK**.

You can view the new policy in the policy management list.

----End

Related Operations

Modifying or deleting a network policy

Step 1 (Optional) If you have enabled the enterprise project, select the enterprise project where the target server resides from the drop-down list.

Step 2 Click **Manage Policy** in the **Operation** column of a cluster using the native Kubernetes network model.

Step 3 Click **Synchronize** above the network policy list.

The synchronization takes about 1 to 2 minutes. Wait for a while and click ⟳ in the upper right corner of the list to refresh and view the latest data.

Step 4 Manage policies as needed.

- Modifying a policy
  - In the **Operation** column of a policy, click **Edit YAML**. On the YAML page, modify the YAML content and click **OK**.
  - In the **Operation** column of a policy, click **Update**. Modify the network policy information and click **OK**.
- Deleting a policy
  - In the **Operation** column of a policy, click **Delete**. In the confirmation dialog box, click **OK**.
  - Select one or multiple policies and click **Delete** above the policy list. In the displayed dialog box, click **OK**.

----End

7.2 Container Cluster Protection

7.2.1 Container Cluster Protection Overview

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.

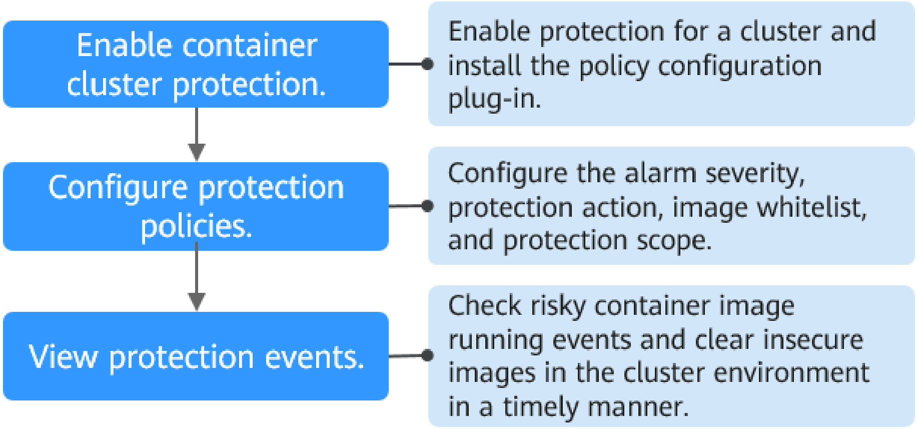
You can configure container cluster protection policies to block images with vulnerabilities, malicious files, non-compliant baselines, or other threats, hardening cluster security.

Constraints

- Container cluster protection is available only in the HSS container edition. For details about how to purchase HSS, see **Purchasing an HSS Quota**.
- To use container cluster protection, ensure the agent installed on the server falls within the following range. For details about how to upgrade the agent, see **Upgrading the Agent**.
  - Linux: 3.2.7 or later
  - Windows: 4.0.19 or later
- The cluster version is 1.20 or later.
- In a CCE cluster, to operate and protect resource objects, you need to obtain either of the following operation permissions:
  - IAM permissions: Tenant Administrator or CCE Administrator.
  - Namespace permissions (authorized by Kubernetes RBAC): O&M permissions. For details about how to configure permissions, see **Configuring namespace permissions**.

Process of Using Container Cluster Protection

Figure 7-9 Usage process



Enable container cluster protection. — Enable protection for a cluster and install the policy configuration plug-in.

Configure protection policies. — Configure the alarm severity, protection action, image whitelist, and protection scope.

View protection events. — Check risky container image running events and clear insecure images in the cluster environment in a timely manner.

Table 7-6 Process of using container cluster protection

Operation	Description
Enable container cluster protection.	Enable protection for a cluster to protect its workloads and critical data. When protection is enabled, HSS automatically installs the policy management plug-in on the cluster.
Configure a protection policy.	Configure the severity of baseline, vulnerability, and malicious file risks that trigger alarms; container cluster protection scope; image whitelist; and actions to be taken on alarms.
Check container cluster protection events.	On the HSS console, you can view unauthorized or high-risk container image running events that are reported or blocked, and check and clear insecure container images in a timely manner.

7.2.2 Enabling Container Cluster Protection

Container cluster protection can detect risks in baselines, vulnerabilities, and malicious files; and can report alarms on or block insecure container images. You can enable protection to enhance cluster defense and protect containers.

Constraints

After container cluster protection is enabled, you need to configure a policy to make the protection take effect. For more information, see **Configuring a Container Cluster Protection Policy**.

Enabling Container Cluster Protection

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

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

Step 3 In the navigation pane, choose > **Container Cluster Protection**.

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

Step 5 Click **Synchronize** to synchronize clusters.

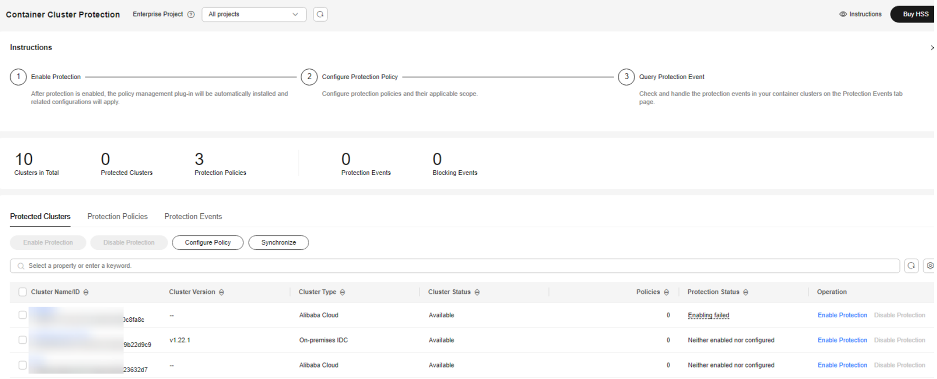
Step 6 Click **Enable** in the **Operation** column of a cluster.

To enable protection for clusters in batches, select clusters and click **Enable Protection** in the upper left corner of the cluster list.

⚠ CAUTION

- After container cluster protection is enabled for a cluster, the policy management plug-in will be installed in the cluster and occupy some cluster resources.
- When enabling protection for a container cluster, do not perform any operation on the cluster. Otherwise, protection will fail to be enabled.

Figure 7-10 Enabling container cluster protection



Container Cluster Protection Enterprise Project All projects Instructions Buy HSS

Instructions

1 Enable Protection
After protection is enabled, the policy management plug-in will be automatically installed and related configurations will apply.

2 Configure Protection Policy
Configure protection policies and their applicable scope.

3 Query Protection Event
Check and handle the protection events in your container clusters on the Protection Events tab page.

10 Clusters in Total
0 Protected Clusters
3 Protection Policies
0 Protection Events
0 Blocking Events

Protected Clusters | Protection Policies | Protection Events

Enable Protection | Disable Protection | Configure Policy | Synchronize

Select a property or enter a keyword.

Cluster Name/ID	Cluster Version	Cluster Type	Cluster Status	Policies	Protection Status	Operation
[redacted] 0c8fa8c	--	Alibaba Cloud	Available	0	Enabling failed	Enable Protection Disable Protection
[redacted] 9b22d9c9	v1.22.1	On-premises IDC	Available	0	Neither enabled nor configured	Enable Protection Disable Protection
[redacted] 23632d7	--	Alibaba Cloud	Available	0	Neither enabled nor configured	Enable Protection Disable Protection

Step 7 Click **OK**.

If the **Protection Status** of the container cluster is **Enabled but not configured**, it indicates protection has been configured for the cluster and the policy management plug-in has been installed, but HSS has not started to protect your cluster. In this case, you need to configure a protection policy. For more information, see **Configuring a Container Cluster Protection Policy**.

----End

7.2.3 Configuring a Container Cluster Protection Policy

You can configure container cluster protection policies to specify the level of risks (unsafe baselines, vulnerabilities, or malicious files) that trigger alarms, cluster protection scope, image whitelist, and the actions taken on an alarm.

Creating a Protection Policy

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

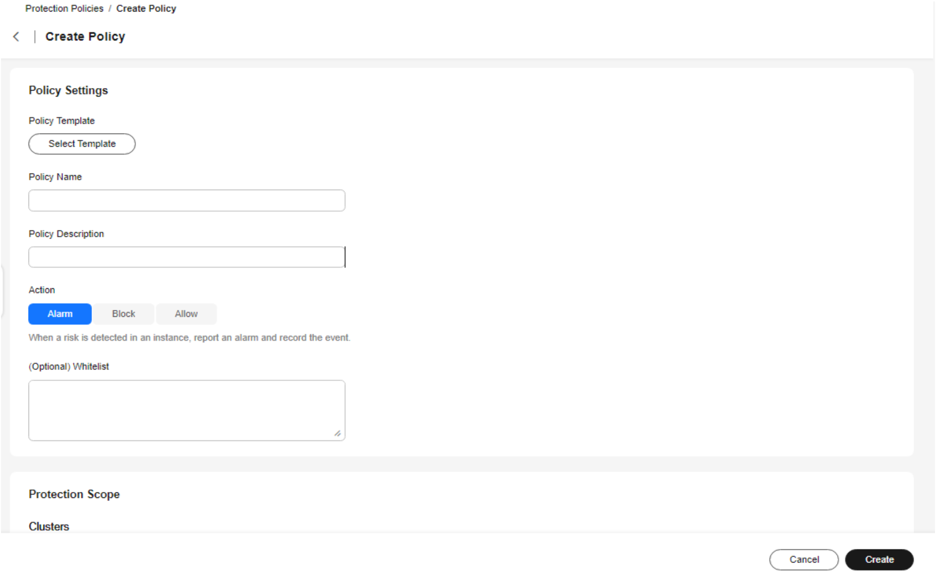
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose > **Container Cluster Protection**.

Step 4 Click the **Protection Policies** tab and click **Create Policy**.

Step 5 In the **Create Policy** dialog box, set policy parameters. For details about related parameters, see **Table 7-7**.

Figure 7-11 Creating a protection policy



When a risk is detected in an instance, report an alarm and record the event.

Table 7-7 Container cluster protection policy parameters

Parameter	Description	Example Value
Policy Template	Select a policy template. The procedure is as follows: 1. Click **Select Template**. 2. Select a policy template and click **OK**. You can select a policy template based on the policy description. After selecting a policy template, configure policy parameters based on the policy template requirements. You can refer to the parameter description.	K8sPSPPrivilegedContainer
Policy Name	Enter a policy name.	test
Policy Description	Enter policy description.	Test

Parameter	Description	Example Value
Action	Action taken by HSS if it detects that an image to be started contains specified unsafe baseline items, vulnerabilities, or malicious scripts. ● **Alarm**: Generate an event whose **Action** is **Alarm** on the **Protection Events** tab of the **Container Cluster Protection** page. ● **Block**: Block an unsafe image and generate an event whose **Action** is **Block** on the **Protection Events** tab of the **Container Cluster Protection** page. ● **Allow**: Generate an event whose **Action** is **Allow** on the **Protection Events** tab of the **Container Cluster Protection** page.	Block
Protection Scope	Configure the protection scope of clusters. If you select the image blocking policy, you need to set the images and tags to specify the protection scope.	-
(Optional) Whitelist	Images to be added to the whitelist. HSS does not check whitelisted images when they are started. Enter values in *ImageName*:*ImageVersion* format. An image name can contain only numbers, letters, underscores (_), hyphens (-), and periods (.). Each image name occupies a separate line. Example: ● A single image **image:1.0** ● Multiple images **image1:1.0** **image2:1.0**	-

Step 6 Click **OK**.

You can view the protection policy in the policy list.

----End

Editing or Deleting a Cluster Protection Policy

Step 1 Choose **Container Cluster Protection** and click the **Protection Policies** tab.

Step 2 In the **Operation** column of a policy, click a button as required.

- **View YAML**: View the protection policy content in YAML format.
- **Edit**: Modify a protection policy.

- **Delete**: Delete a protection policy. After a policy is deleted, the container clusters associated with it will no be protected. Exercise caution when performing this operation.

Step 3 Click **OK**.

----End

7.2.4 Checking Container Cluster Protection Events

HSS detects risks and displays security events in the protection event list. This section describes how to check the events.

Checking Container Cluster Protection Events

Step 1 Log in to the management console.

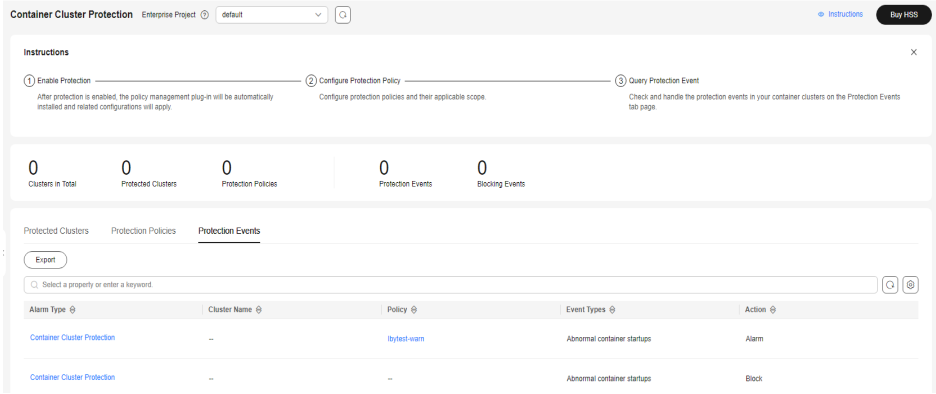
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose > **Container Cluster Protection**.

Step 4 Click the **Protection Events** tab and check events in the cluster.

To export events to your local PC, click **Export** in the upper left corner of the event list.

Figure 7-12 Viewing protection events



1. Enable Protection
   After protection is enabled, the policy management plug-in will be automatically installed and related configurations will apply.
2. Configure Protection Policy
   Configure protection policies and their applicable scope.
3. Query Protection Event
   Check and handle the protection events in your container clusters on the Protection Events tab page.

Alarm Type	Cluster Name	Policy	Event Types	Action
Container Cluster Protection	--	lbytest-warn	Abnormal container startups	Alarm
Container Cluster Protection	--	--	Abnormal container startups	Block

Step 5 Click an alarm name to view affected resources.

----End

7.2.5 Disabling Container Cluster Protection

If you no longer need HSS to protect your container clusters, you can disable container cluster protection.

Disabling Container Cluster Protection

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose > **Container Cluster Protection**.

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

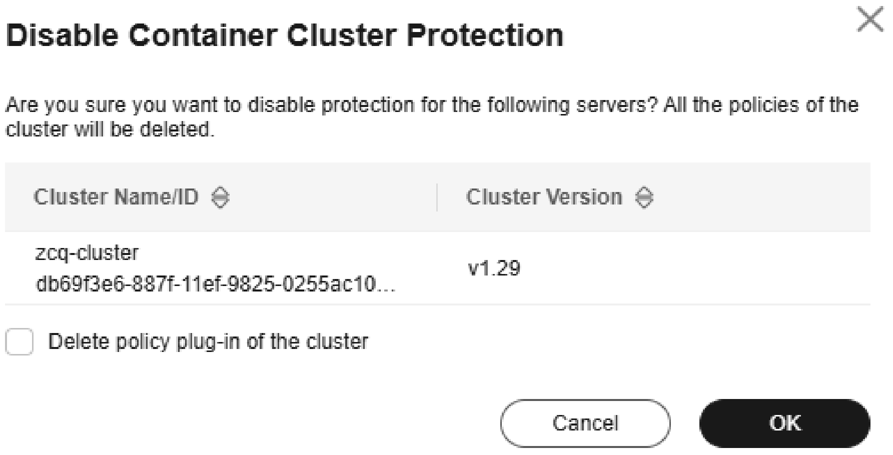
Step 5 In the **Operation** column of a cluster, click **Disable Protection**.

To disable protection for clusters in batches, select clusters and click **Disable Protection** in the upper left corner of the cluster list.

Step 6 In the dialog box that is displayed, determine whether to select the **Delete policy plug-in of the cluster** check box.

- If you select it, container cluster protection policies and the policy configuration plug-in will be deleted. If you enable protection again, you will need to install the policy configuration plug-in and configure protection policies again.
- If you deselect it, container cluster protection policies will be deleted but the policy configuration plug-in will be retained. If you enable protection again, you only need to configure protection policies. If you want to delete the policy configuration plug-in later, repeat the preceding steps to disable protection and select **Delete policy plug-in of the cluster**.

Figure 7-13 Disabling container cluster protection



Disable Container Cluster Protection

Are you sure you want to disable protection for the following servers? All the policies of the cluster will be deleted.

Cluster Name/ID	Cluster Version
zcq-cluster db69f3e6-887f-11ef-9825-0255ac10...	v1.29

□ Delete policy plug-in of the cluster

Step 7 Click **OK**.

- If you did not select **Delete policy plug-in of the cluster** and the **Protection Status** of the cluster changes to **Enabled but not configured**, it indicates protection has been disabled.
- If you selected **Delete policy plug-in of the cluster** and the **Protection Status** of the cluster changes to **Unprotected**, it indicates protection has been disabled.

----End

FAQ

If the cluster network is abnormal or the plug-in is working, you will probably fail to uninstall the plug-in on the HSS console. In this case, you can refer to the content below: **What Do I Do If the Container Cluster Protection Plug-in Fails to Be Uninstalled?**

8 Detection and Response

8.1 HSS Alarms

8.1.1 Server Alarms

HSS generates alarms on a range of intrusion events, including brute-force attacks, abnormal process behaviors, web shells, abnormal logins, and malicious processes. You can learn all these events on the console, and eliminate security risks in your assets in a timely manner.

NOTE

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

Constraints

Servers that are not protected by HSS do not support alarm-related operations.

Server Security Alarms

For details about server security alarm types and alarm items, see **Table 8-1**. Alarms vary by HSS edition. For details, see **Features**.

Malicious files or processes can be isolated and removed manually or automatically. **Enable automatic isolation and killing** as needed. If a program is isolated and killed, its process will be terminated immediately. To avoid impact on services, exercise caution when performing this operation. If this function is enabled, check scan results in a timely manner, and cancel the incorrect isolation of files.

Table 8-1 Server security alarms

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Malware	Malicious software includes viruses, worms, Trojans, and web shells implanted by hackers to steal your data or control your servers. For example, hackers will probably use your servers as miners or DDoS zombies. This occupies a large number of CPU and network resources, affecting service stability.	Unclassified malware	Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants, and kill them in one-click. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing. **Supported OSs**: Linux and Windows. **Isolation and removal**: automated or manual
		Viruses	Detect diverse viruses in server assets, reports alarms, and isolate and remove virus files. **Supported OSs**: Linux and Windows. **Isolation and removal**: automated or manual
		Worms	Detect and kill worms on servers and report alarms. **Supported OSs**: Linux and Windows. **Isolation and removal**: automated or manual
		Trojans	Detect and remove Trojan and viruses on servers and report alarms. **Supported OSs**: Linux and Windows. **Isolation and removal**: automated or manual
		Botnets	Detect and kill botnets on servers and report alarms. **Supported OSs**: Linux and Windows. **Isolation and removal**: automated or manual

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Backdoors	Detect backdoors in servers and reports alarms. **Supported OSs**: Linux and Windows. **Isolation and removal**: automated or manual
		Rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders. **Supported OSs**: Linux.
		Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion. **Supported OSs**: Linux and Windows. **Isolation and killing**: Automatically or manually detect, isolate, and remove some ransomware.
		Hacker tools	Detect and kill hacker tools on servers and report alarms. **Supported OSs**: Linux and Windows. **Isolation and removal**: manual

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Web shells	Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. You can configure the web shell detection rule in the **Web Shell Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands. You need to add a protected directory in policy management. For details, see **Web Shell Detection**. **Supported OSs**: Linux and Windows. **Isolation and removal**: automated or manual
		Mining software	Detect, scan, and remove mining software on servers, and report alarms. **Supported OSs**: Linux and Windows. **Isolation and removal**: automated or manual

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Vulnerability Exploits	The exploit of vulnerabilities in the server system, software, or network to obtain unauthorized access rights, steal data, or damage the target system. Exploits can be performed remotely or locally. In a remote vulnerability exploit, an attacker connects to the target system through the network and discovers system vulnerabilities to launch attacks. In a local vulnerability exploit, an attacker obtains low access permissions on the target system and exploits vulnerabilities to escalate permissions or perform other malicious operations.	Remote code executions	Detect and report alarms on server intrusions that exploit vulnerabilities in real time. **Supported OSs**: Linux and Windows.
		Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms. **Supported OSs**: Linux.
		Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms. **Supported OSs**: Linux.
		MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms. **Supported OSs**: Linux.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Abnormal System Behaviors	Abnormal system behaviors occur while servers are running, and are usually caused by system faults, malicious attacks, or security vulnerabilities. Abnormal system behaviors may cause data loss or system breakdown. To protect server system and data security, it is important to detect and handle abnormal system behaviors in a timely manner.	Reverse shells	Monitor user process behaviors in real time to report alarms on and block reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. You can configure the reverse shell detection rule in the **Malicious File Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands. To enable automatic reverse shell blocking, enable **Auto Blocking** in the **HIPS Detection** policy on the **Policies** page. Currently, the following types of reverse shells can be blocked: exec reverse shell, Perl reverse shell, AWK reverse shell, Python reverse shell.b, Python reverse shell.a, Lua reverse shell, mkfifo/openssl reverse shell, PHP reverse shell, Ruby reverse shell, rssocks reverse proxy, Bash reverse shell, Ncat reverse shell, exec redirection reverse shell, Node reverse shell, Telnet dual-port reverse shell, nc reverse shell, Socat reverse shell, rm/mkfifo/sh/nc reverse shell, and socket/tchsh reverse shell. **Supported OSs**: Linux.
		File privilege escalations	Detect file privilege escalation behaviors and generate alarms. **Supported OSs**: Linux.
		Process privilege escalations	Detect the privilege escalation operations of the following processes and generate alarms: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities **Supported OSs**: Linux.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Important file changes	Monitor important system files (such as ls, ps, login, and top) in real time and generate alarms if these files are modified. For details about the monitored paths, see **Monitored Important File Paths**. HSS reports all the changes on important files, regardless of whether the changes are performed manually or by processes. **Supported OSs**: Linux.
		File/Directory changes	Monitor system files and directories in real time and generate alarms if such files are created, deleted, moved, or if their attributes or content are modified. **Supported OSs**: Linux and Windows.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following anomalies can be detected: ● Abnormal process path: A process path containing abnormal marks, such as hidden, temporary, and file deletion records. Scored 1 to 3 points. ● Abnormal process connection: Access to malicious IP addresses. Scored 3 to 6 points. ● Process CPU exception: Abnormal CPU usage of a process. Scored 1 point. ● Abnormal executable file of a process: A process executable file containing abnormal characters. Scored 3 points. If the total score of abnormal processes is greater than or equal to 3, an alarm is reported, and the matched rules and their scores are displayed. **Supported OSs**: Linux and Windows. **Isolation and killing**: Some abnormal processes can be manually isolated and killed.
		High-risk command executions	You can configure what commands will trigger alarms in the **High-risk Command Scan** rule on the **Policies** page. HSS checks executed commands in real time and generates alarms if high-risk commands are detected. **Supported OSs**: Linux and Windows.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Abnormal shells	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. You can configure the abnormal shell detection rule in the **Malicious File Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands. **Supported OSs**: Linux.
		Sensitive file access detection	Detect the unauthorized access to or modifications of sensitive files. **Supported OSs**: Linux and Windows.
		Suspicious crontab tasks	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans. **Supported OSs**: Linux and Windows.
		System protection disabling	Detect the preparations for ransomware encryption: Disable the Windows defender real-time protection function through the registry. Once the function is disabled, an alarm is reported immediately. **Supported OSs**: Windows.
		Backup deletion	Detect the operations performed by ransomware before it encrypts your data. Once HSS detects that backup files or files in the **Backup** folder are deleted, an alarm is reported. **Supported OSs**: Windows.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Suspicious registry operations	Detect operations such as disabling the system firewall through the registry and using the ransomware **Stop** to modify the registry and write specific strings in the registry. An alarm is reported immediately when such operations are detected. **Supported OSs**: Windows.
		System log deletion	An alarm is generated when a command or tool is used to clear system logs. **Supported OSs**: Windows.
		Suspicious command executions	● Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. ● Detect suspicious remote command execution. **Supported OSs**: Windows.
		Suspicious process executions	If application process control is enabled, HSS checks for application processes that are not authenticated or authorized based on the whitelist policy, and reports an alarm if such a process is detected. For more information, see **Application Process Control Overview**. **Supported OSs**: Linux and Windows.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Suspicious process file access	If application process control is enabled, HSS checks for application processes that access specified directories but are not authenticated or authorized based on the whitelist policy, and reports an alarm if such a process is detected. For more information, see **Application Process Control Overview**. **Supported OSs**: Linux and Windows.
		Kernel module loading	Check for kernel module loading and reports an alarm immediately when loading is detected. In kernel module loading, a precompiled kernel module (.ko file) is loaded to a running Linux kernel by using commands such as **insmod** and **modprobe** to extend kernel functions. If kernel modules are loaded without strict security reviews, hackers may use the kernel modules to inject malicious code and escalate permissions. This may interfere with kernel operations and even lead to system breakdown. **Supported OSs**: Linux.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Abnormal User Behaviors	Abnormal or unexpected user behaviors that occur in a specific environment or system, sometimes within a short period of time, such as abnormal logins or unauthorized access. To detect and identify these abnormal behaviors, user operations need to be checked and analyzed.	Brute-force attacks	If hackers log in to your servers through brute-force attacks, they can obtain the control permissions of the servers and perform malicious operations, such as steal user data; implant ransomware, miners, or Trojans; encrypt data; or use your servers as zombies to perform DDoS attacks. HSS can detect brute-force attacks on the following service accounts: ● Windows: RDP, SQL Server ● Linux: MySQL, vsftpd, SSH If five or more consecutive incorrect passwords are entered from the same IP address within 30 seconds, or the total number of incorrect passwords entered from the same IP address reaches 15 within 1 hour, HSS will generate an alarm for the latest user who entered an incorrect password from the IP address, and will block the IP address (for 12 hours by default) to prevent server intrusions caused by brute-force attacks. You can check whether a login IP address can be trusted based on its brute-force attack alarm details, including the attack source IP address, attack type, and how many times it has been blocked. You can manually unblock trusted IP addresses. **Supported OSs**: Linux (excluding Debian 12, Ubuntu 24.04, and SUSE 15 SP6) and Windows

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Abnormal logins	Detect abnormal login behavior, such as remote login and brute-force attacks. If abnormal logins are reported, your servers may have been intruded by hackers. ● Check and handle remote logins. You can check the blocked login IP addresses, and who used them to log in to which server at what time. If a user's login location is not any common login location, an alarm will be triggered. ● Trigger an alarm if a user logs in to the server by a brute-force attack. **Supported OSs**: Linux and Windows.
		Invalid accounts	Hackers can probably crack unsafe accounts on your servers and control the servers. HSS checks suspicious hidden accounts and cloned accounts and generates alarms on them. **Supported OSs**: Linux and Windows.
		User account added	Detect the commands used to create hidden accounts. Hidden accounts cannot be found in the user interaction interface or be queried by commands. **Supported OSs**: Windows.
		Password thefts	Detect the abnormal obtaining of hash value of system accounts and passwords on servers and report alarms. **Supported OSs**: Windows.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Abnormal Network Access	Abnormal network access refers to exceptions that occur during network connection or data transmission and different from normal usage. These exceptions include abnormal resource usage, unauthorized access, and abnormal connections. Abnormal network access behaviors on servers may be a prelude to attacks.	Cloud honeypots	An alarm is reported if a connection to the honeypot port of a server is detected. **Supported OSs**: Linux and Windows.
		Suspicious download requests	An alarm is generated when a suspicious HTTP request that uses system tools to download programs is detected. **Supported OSs**: Windows.
		Suspicious HTTP requests	An alarm is generated when a suspicious HTTP request that uses a system tool or process to execute a remote hosting script is detected. **Supported OSs**: Windows.
		Abnormal outbound connections	Report alarms on suspicious IP addresses that initiate outbound connections. **Supported OSs**: Linux (kernel 5.10 or later).
		Port forwarding	Report alarms on port forwarding using suspicious tools. **Supported OSs**: Linux.
Reconnaissance	Reconnaissance is the act of gathering information about a target network before launching an attack.	Port scans	Detect scanning or sniffing on specified ports and report alarms. **Supported OSs**: Linux.
		Server scans	Detect the network scan activities based on server rules (including ICMP, ARP, and nbtscan) and report alarms. **Supported OSs**: Linux.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Fileless Attacks	A fileless attack does not release malicious executable files. Instead, it writes malicious code into the system memory or registry. Because there are no malicious files used, such an attack is difficult to detect. Fileless attacks are classified into the following types based on disk file activities: ● No file activities. That is, no disk files are stored or operated in disks. Generally, such attacks are initiated in the upper-layer hardware, firmware, or software layer rather than the OS. ● Indirect activities through files. That is, no files are stored in disks, but activities are indirectly performed through files. Malicious code is usually indirectly loaded to the memory for execution through white files. Most of such malicious code is carried by scripts, which are executed through program commands or specific mechanisms such as disk boot records. ● File activities required.	Process injection	Scan for malicious code injection into running processes and report alarms. **Supported OSs**: Linux.
		Dynamic library injection	Scan for the payloads injected by hijacking functions in the dynamic link library (DLL) and report alarms. **Supported OSs**: Linux.
		Memory file processes	Scan for the behaviors of creating an anonymous malicious file that exists only in the RAM through the memfd_create system call and executing the file, and report alarms on such behaviors. **Supported OSs**: Linux.
		VDSO hijacking	Scan for the attacks that exploit specific vulnerabilities (for example, Dirty COW). Such attacks overwrite the original code of VDSO with malicious code. If the root process calls the code of the VDSO, the malicious code will be executed and privilege escalation will be performed. An alarm will be reported immediately if such an attack is detected. **Supported OSs**: Linux.
		Windows tool exploits	Scan for the attacks that exploit the legitimate built-in tools and functions in the OS to perform malicious operations that can bypass the traditional security defense mechanism. An alarm will be reported immediately if such an attack is detected. **Supported OSs**: Windows.
		Malicious registry injection	Scan for the attacks that insert malicious code or scripts into the Windows registry, which enables malware to automatically run when the system is started and bypass the common file detection

Alarm Type	Alarm Type Description	Alarm	Alarm Description
	Generally, malicious code is converted into data. Attackers exploit file-related program vulnerabilities or features to convert malicious data into malicious code for execution.		mechanism. An alarm will be reported immediately if such an attack is detected. **Supported OSs**: Windows.

Security Alarm Severities

HSS alarm severities indicate alarm impact on service systems. It can be Critical, High, Medium, or Low. For details, see **Table 8-2**.

Table 8-2 Security alarm severities

Alarm Severity	Description
Critical	A critical alarm indicates that the system is severely attacked, which may cause data loss, system breakdown, or long service interruption. For example, such alarms are generated if ransomware encryption behaviors or malicious programs are detected. You are advised to handle the alarms immediately to avoid severe system damage.
High	A high-risk alarm indicates that the system may be under an attack that has not caused serious damage. For example, such alarms are generated if unauthorized login attempts are detected or unsafe commands (for deleting critical system files or modifying system settings) are executed. You are advised to investigate and take measures in a timely manner to prevent attacks from spreading.
Medium	A medium-risk alarm indicates that the system has potential security threats, but there are no obvious signs of being attacked. For example, if abnormal modifications of a file or directory are detected, there may be potential attack paths or configuration errors in the system. You are advised to further analyze and take proper preventive measures to enhance system security.

Alarm Severity	Description
Low	A low-risk alarm indicates that a minor security threat exists in the system but does not have significant impact on your system. For example, such alarms are generated if port scans are detected, indicating that there may be attackers trying to find system vulnerabilities. These alarms do not require immediate emergency measures. If you have high requirements on asset security, pay attention to the security alarms of this level.

Monitored Important File Paths

Type	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

8.1.2 Viewing Server Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of urgent alarms, total alarms, servers with alarms, blocked IP addresses, and isolated files.

The **Events** page displays the alarm events generated in the last 30 days. You can manually handle the alarmed items.

The status of a handled event changes from **Unhandled** to **Handled**.

NOTE

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

Constraints

- To skip the checks on high-risk command execution, privilege escalations, reverse shells, abnormal shells, or web shells, manually disable the corresponding policies in the policy groups on the **Policies** page. HSS will not check the servers associated with disabled policies. For details, see **Viewing a Policy Group**.
- Other detection items cannot be manually disabled.
- Servers that are not protected by HSS do not support operations related to alarms and events.

Viewing Server Alarms

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

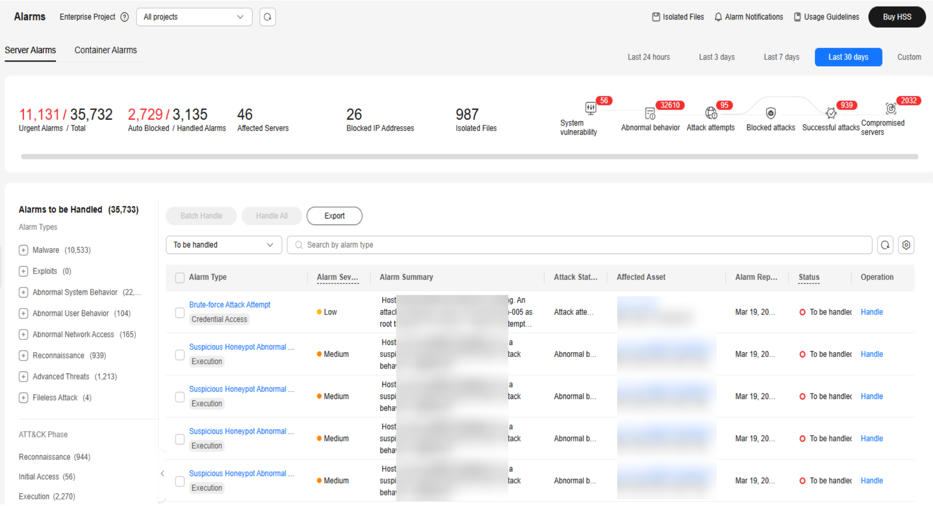
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Detection & Response** > **Alarms** and click **Server Alarms**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Check server alarms.

Figure 8-1 Server alarms



11,131 / 35,732 Urgent Alarms / Total
2,729 / 3,135 Auto Blocked / Handled Alarms
46 Affected Servers
26 Blocked IP Addresses
987 Isolated Files

System vulnerability 56
Abnormal behavior 32610
Attack attempts 95
Blocked attacks
Successful attacks 939
Compromised servers 2032

Alarms to be Handled (35,733)

Alarm Types
- Malware (10,533)
- Exploits (0)
- Abnormal System Behavior (22,...
- Abnormal User Behavior (104)
- Abnormal Network Access (165)
- Reconnaissance (939)
- Advanced Threats (1,213)
- Fileless Attack (4)

ATT&CK Phase
- Reconnaissance (944)
- Initial Access (56)
- Execution (2,270)

□ Alarm Type	Alarm Sev...	Alarm Summary	Attack Stat...	Affected Asset	Alarm Rep...	Status	Operation
□ Brute-force Attack Attempt Credential Access	● Low	Host attacl root t [redacted] g. An -005 as tempt...	Attack atte...	[redacted]	Mar 19, 20...	○ To be handled	Handle
□ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handled	Handle
□ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handled	Handle
□ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handled	Handle
□ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handled	Handle

Table 8-3 Alarm statistics

Parameter	Description
Enterprise Project	Select an enterprise project and view alarm details by enterprise project.
Time range	You can select a fixed period or customize a time range to search for alarms. Only alarms generated within 30 days can be queried. The options are as follows: ● Last 24 hours ● Last 3 days ● Last 7 days ● Last 30 days
Urgent Alarms / Total	Number of alarms to be handled and total number of alarms. You can click a number to view the alarm list.
Auto Blocked / Handled Alarms	Number of blocked alarms and number of handled alarms. Click a number to view the alarm list.
Affected Servers	Number of servers that trigger alarms. You can click a number to go to the **Servers & Quota** page and view the server list. When checking alarms generated in the last 24 hours, you can click the number of servers to go to the **Servers & Quota** page and check the corresponding servers.
Blocked IP Addresses	Number of blocked brute-force attack IP addresses. You can click the number to check blocked IP address list. The blocked IP address list displays the server name, attack source IP address, login type, blocking status, number of blocks, blocking start time, and the latest blocking time. If a valid IP address is blocked by mistake (for example, after O&M personnel enter incorrect passwords for multiple times), you can manually unblock it. If a server is frequently attacked, you are advised to fix its vulnerabilities in a timely manner and eliminate risks. Notes: ● The agent of Linux 3.2.10 or later supports IPv6 blocking. The agent of any earlier version can use TCP Wrapper for blocking, but cannot use iptables for IPv6 blocking. ● After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address. ● A maximum of 10,000 IP addresses can be blocked for each type of software. If your Linux server does not support ipset, a maximum of 50 IP addresses can be blocked for MySQL and vsftp. If your Linux server does not support ipset or hosts.deny, a maximum of 50 IP addresses can be blocked for SSH.

Parameter	Description
Isolated Files	HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** page. You can click **Isolated Files** on the upper right corner to check them. You can recover isolated files. For details, see **Managing Isolated Files**. You can click the number under **Isolated Files** to check the files.

- **Viewing the alarms of a certain type or ATT&CK phase**

  In the **Alarms to Be Handled** area, you can select an alarm type and an ATT&CK phase to view the alarms of the selected type. For details, see **ATT&CK attack phase description**.

  NOTE

  Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a framework that helps organizations understand the cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle.

  Table 8-4 ATT&CK phases

ATT&CK Phase	Description
Reconnaissance	Attackers seek vulnerabilities in your system or network.
Initial Access	Attacker try to enter your system or network.
Execution	Attackers try to run malicious code.
Persistence	Attackers try to maintain their foothold.
Privilege Escalation	Attackers try to obtain higher permissions.
Defense Evasion	Attackers try to avoid being detected.
Credential Access	Attackers try to steal account names and passwords.
Command and Control	Attackers try to communicate with compromised machines to control them.
Impact	Attackers try to manipulate, interrupt, or destroy your system or data.

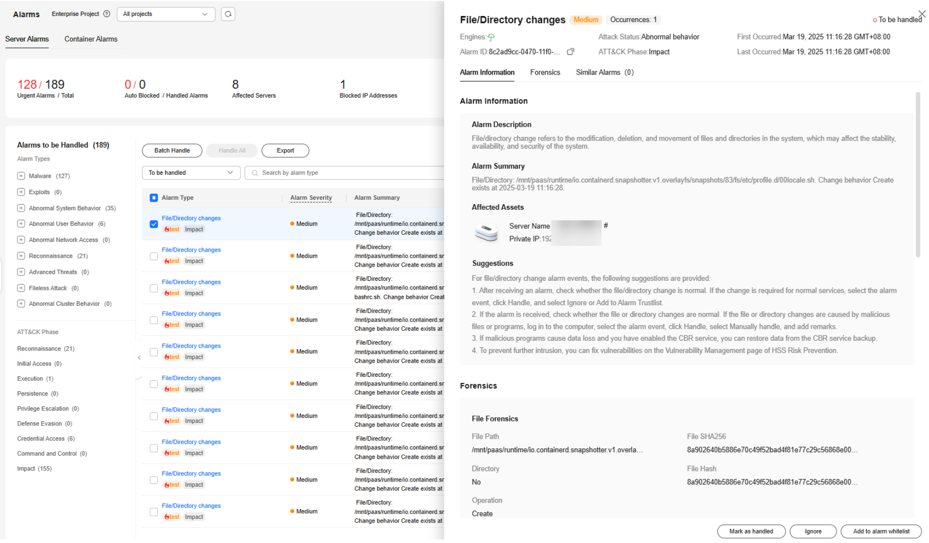
- **Viewing the details of a server alarm**

  You can click the alarm name of an event to view the alarm details. **Table 8-5** describes the alarm parameters.

NOTE

- For some HSS alarms that have been determined as malware alarms, the alarm source files are saved in the cloud center and you can download them. You can download the alarm source files to your local PC for analysis. The password for decompressing the files is **unlock**.
- For unacknowledged malware alarms, alarm source files cannot be downloaded. Check the actual service conditions and determine whether the files are malicious files.

Figure 8-2 Alarm details



128 / 189 Urgent Alarms / Total
0 / 0 Auto Blocked / Handled Alarms
8 Affected Servers
1 Blocked IP Addresses

Alarms to be Handled (189)

Alarm Types
- Malware (127)
- Exploits (0)
- Abnormal System Behavior (35)
- Abnormal User Behavior (6)
- Abnormal Network Access (0)
- Reconnaissance (21)
- Advanced Threats (0)
- Fileless Attack (0)
- Abnormal Cluster Behavior (0)

ATT&CK Phase
- Reconnaissance (21)
- Initial Access (0)
- Execution (1)
- Persistence (0)
- Privilege Escalation (0)
- Defense Evasion (0)
- Credential Access (6)
- Command and Control (0)
- Impact (155)

☑ Alarm Type	Alarm Severity	Alarm Summary
☑ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr Change behavior Create exists at
□ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr Change behavior Create exists at
□ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr bashrc.sh. Change behavior Creat
□ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr Change behavior Create exists at
□ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr Change behavior Create exists at
□ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr Change behavior Create exists at
□ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr Change behavior Create exists at
□ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr Change behavior Create exists at
□ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr Change behavior Create exists at
□ File/Directory changes test Impact	● Medium	File/Directory: /mnt/paas/runtime/io.containerd.sr Change behavior Create exists at

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

Engines:
Attack Status:Abnormal behavior
First Occurred:Mar 19, 2025 11:16:28 GMT+08:00
Alarm ID:8c2ad9cc-0470-11f0-...
ATT&CK Phase:Impact
Last Occurred:Mar 19, 2025 11:16:28 GMT+08:00

Alarm Information | Forensics | Similar Alarms (0)

Alarm Information

Alarm Description

File/directory change refers to the modification, deletion, and movement of files and directories in the system, which may affect the stability, availability, and security of the system.

Alarm Summary

File/Directory: /mnt/paas/runtime/io.containerd.snapshotter.v1.overlayfs/snapshots/83/fs/etc/profile.d/00locale.sh. Change behavior Create exists at 2025-03-19 11:16:28.

Affected Assets

Server Name [redacted] #
Private IP:192

Suggestions

For file/directory change alarm events, the following suggestions are provided:
1. After receiving an alarm, check whether the file/directory change is normal. If the change is required for normal services, select the alarm event, click Handle, and select Ignore or Add to Alarm Trustlist.
2. If the alarm is received, check whether the file or directory changes are normal. If the file or directory changes are caused by malicious files or programs, log in to the computer, select the alarm event, click Handle, select Manually handle, and add remarks.
3. If malicious programs cause data loss and you have enabled the CBR service, you can restore data from the CBR service backup.
4. To prevent further intrusion, you can fix vulnerabilities on the Vulnerability Management page of HSS Risk Prevention.

Forensics

File Forensics

File Path: /mnt/paas/runtime/io.containerd.snapshotter.v1.overla...
File SHA256: 8a902640b5886e70c49f52bad4f81e77c29c56868e00...
Directory: No
File Hash: 8a902640b5886e70c49f52bad4f81e77c29c56868e00...
Operation: Create

Table 8-5 Alarm detail parameters

Parameter	Description
Protection Engine	Detection engines used by HSS, including the virus detection engine, AI detection engine, and malicious intelligence detection engine.
Attack Status	Status of the current threat.
First Occurred	Time when an attack alarm was first generated
Alarm ID	Unique ID of an alarm
ATT&CK Phase	For details about the attack technology models used by attackers in each phase, see **Table 8-4**.
Last Occurred	Time when an attack alarm was last generated
Alarm Information	Detailed information about an alarm, including the alarm description, alarm summary, affected assets, and handling suggestions.

Parameter	Description
Forensics	HSS investigates information such as the attack triggering path or virus type based on the alarm type, helping you quickly trace and locate the attack source. – **Process Tree**: If an alarm event contains process information, you can check the process ID, process file path, process command line, process startup time, and process file hash on the **Forensics** tab page. You can locate malicious processes based on such information. – **File Forensics**: If an alarm event contains file information, the file forensics information is displayed on the **Forensics** tab page. File forensics information includes the file path, file hash, file operation type, and user information (which may not be obtained by instantaneous processes). You can locate a file based on the information. – Network Forensics: If an alarm event contains file information, the network forensics information is displayed on the **Forensics** tab page. Network forensics information includes the local IP address, local port, remote IP address, remote port, and protocol. You can determine whether the access is unauthorized based on such information. – User Forensics: If an alarm event contains user behavior information, the user forensics information is displayed on the **Forensics** tab page. User forensics information includes the username, login IP address, login service type, login service port, last login event, and number of login failures. You can determine whether the access is unauthorized based on such information. – **Registry Forensics**: If an alarm event contains registry information, you can check the registry keys and values on the **Forensics** tab page. You can locate registry risks based on such information. – **Abnormal Login Forensics**: If an alarm event contains abnormal login information, you can check the login IP address and port number on the **Forensics** tab page. You can determine whether the login is trusted based on such information. – **Malware Forensics**: If an alarm event contains malware information, you can check the malware family, virus name, virus type, and confidence level on the **Forensics** tab page. – **Auto-started Item Forensics**: If an alarm event contains self-startup item information, you can check the user, command, self-startup item information, and process file command line information on the **Forensics** tab page. You can locate the auto-boot item based on the auto-started item forensics information. – **Kernel Forensics**: If an alarm event contains kernel information, you can check system functions and kernel

Parameter	Description
	functions on the **Forensics** tab page. You can locate kernel risks based on the information.
Similar Alarms	Alarm whose server and event type are the same as those of this alarm. You can handle the alarm according to the handling method of the similar alarms.

----End

FAQ

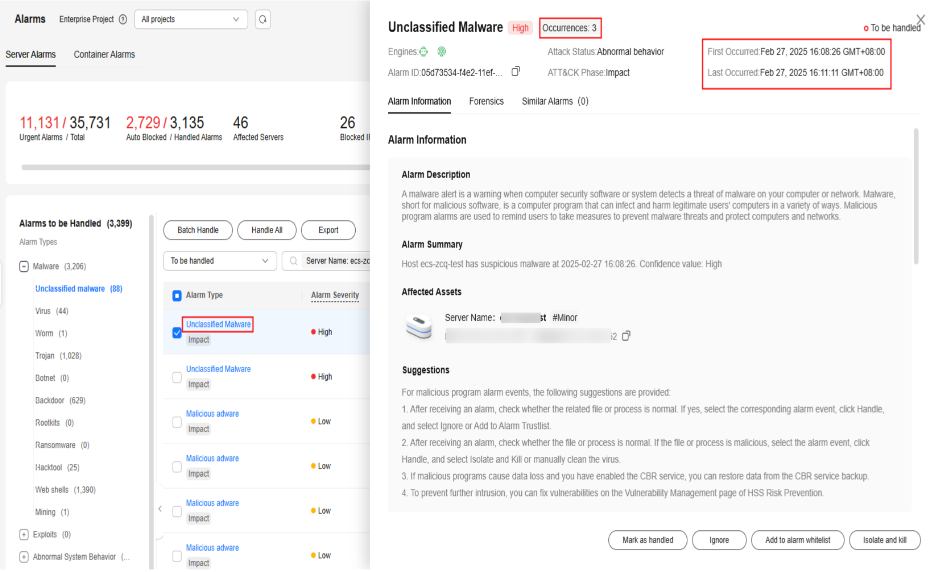
- **Why are there multiple similar alarms?**

  If similar events that occur within 24 hours, HSS combines them into one alarm. If similar events occur at an interval of 24 hours or more, HSS reports them as independent alarms. Therefore, you can see multiple similar alarms.

- **How do I check the number of similar alarms that occurred within 24 hours?**

  Click an alarm name to view the number of occurrences, first occurrence time, and latest occurrence time on the alarm details page.

Figure 8-3 Alarm details



Engines:

Attack Status:Abnormal behavior

First Occurred:Feb 27, 2025 16:08:26 GMT+08:00

Alarm ID:05d73534-f4e2-11ef-...

ATT&CK Phase:Impact

Last Occurred:Feb 27, 2025 16:11:11 GMT+08:00

Alarm Information

Alarm Description

A malware alert is a warning when computer security software or system detects a threat of malware on your computer or network. Malware, short for malicious software, is a computer program that can infect and harm legitimate users' computers in a variety of ways. Malicious program alarms are used to remind users to take measures to prevent malware threats and protect computers and networks.

Alarm Summary

Host ecs-zcq-test has suspicious malware at 2025-02-27 16:08:26. Confidence value: High

Affected Assets

Server Name: [redacted]st #Minor

[redacted]2

Suggestions

For malicious program alarm events, the following suggestions are provided:

1. After receiving an alarm, check whether the related file or process is normal. If yes, select the corresponding alarm event, click Handle, and select Ignore or Add to Alarm Trustlist.
2. After receiving an alarm, check whether the file or process is normal. If the file or process is malicious, select the alarm event, click Handle, and select Isolate and Kill or manually clean the virus.
3. If malicious programs cause data loss and you have enabled the CBR service, you can restore data from the CBR service backup.
4. To prevent further intrusion, you can fix vulnerabilities on the Vulnerability Management page of HSS Risk Prevention.

8.1.3 Handling Server Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of urgent alarms, total alarms, servers with alarms, blocked IP addresses, and isolated files.

The **Events** page displays the alarms generated in the last 30 days.

The status of a handled alarm changes from **Unhandled** to **Handled**.

NOTE

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

Constraints

- To skip the checks on high-risk command execution, privilege escalations, reverse shells, abnormal shells, or web shells, manually disable the corresponding policies in the policy groups on the **Policies** page. HSS will not check the servers associated with disabled policies. For details, see **Viewing a Policy Group**.
- Other detection items cannot be manually disabled.
- Servers that are not protected by HSS do not support operations related to alarms and events.
- Alarms reported by the graph engine cannot be handled in batches.

Handling Server Alarms

This section describes how you should handle alarms to enhance server security.

NOTE

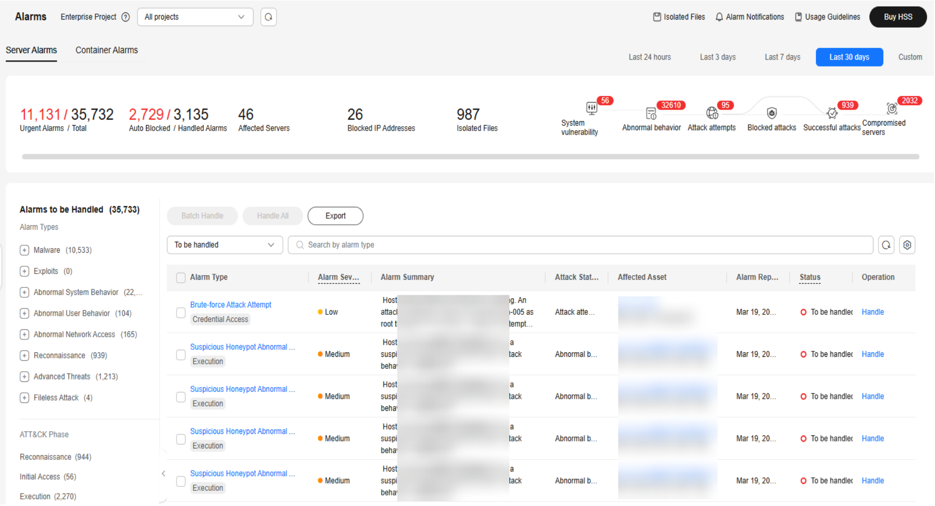
Do not fully rely on alarm handling to defend against attacks, because not every issue can be detected in a timely manner. You are advised to take more measures to prevent threats, such as checking for and fixing vulnerabilities and unsafe settings.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Detection & Response** > **Alarms** and click **Server Alarms**.

Figure 8-4 Server alarms



□ Alarm Type	Alarm Sev...	Alarm Summary	Attack Stat...	Affected Asset	Alarm Rep...	Status	Operation
□ Brute-force Attack Attempt Credential Access	● Low	Host attac root t [redacted] g. An -005 as tempt...	Attack atte...	[redacted]	Mar 19, 20...	○ To be handlec	Handle
□ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handlec	Handle
□ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handlec	Handle
□ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handlec	Handle
□ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handlec	Handle

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click an alarm name to view the alarm details and suggestions.

Step 6 Handle alarms.

Check and handle alarms as needed. The status of a handled alarm changes from **Unhandled** to **Handled**.

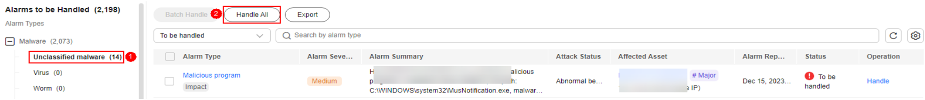
- Handling a single alarm

  In the **Operation** column of an alarm, click **Handle**.
- Handling alarms in batches

  Select all alarms and click **Batch Handle** above the alarm list.
- Handling all alarms

  In the **Alarms to be Handled** area on the left pane of the alarm list, select an alarm type and click **Handle All** above the alarm list.

Figure 8-5 Handling all alarms



Alarm Type	Alarm Seve...	Alarm Summary	Attack Status	Affected Asset	Alarm Rep...	Status	Operation
Malicious program Impact	Medium	[redacted] alicious C:\WINDOWS\system32\MusNotification.exe, malwar...	Abnormal be...	[redacted] # Major	Dec 15, 2023...	To be handled	Handle

Step 7 In the **Handle Event** dialog box, select an action. For details about the alarm handling actions, see **Table 8-6**.

When you handle one or multiple alarm events, you can select **Handle duplicate alarms in batches** in the **Handle Event** dialog box.When handling a graph engine alarm, you can select different handling methods for different suspicious processes or files.

Table 8-6 Alarm handling methods

Action	Description
Ignore	Ignore the current alarm. Any new alarms of the same type will still be reported by HSS.
Isolate and kill	If a program is isolated and killed, it will be terminated immediately and no longer able to perform read or write operations. Isolated source files of programs or processes are displayed on the **Isolated Files** slide-out panel and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check the files. For details, see **Managing Isolated Files**. For details about events that can be isolated and killed, see **Server Alarms**. **NOTE** When a program is isolated and killed, the process of the program is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious programs (if any).

Action	Description
Mark as handled	If you have manually handled an event, choose **Mark as handled**. You can add remarks to record details about event handling.
Add to process whitelist	If you can confirm that a process triggering an alarm can be trusted, you can add it to the process whitelist. HSS will no longer report alarms on whitelisted processes.
Add to Login Whitelist	Add false alarmed items of the **Brute-force attack** and **Abnormal login** types to the Login Whitelist. HSS will no longer report alarm on the Login Whitelist. A whitelisted login event will not trigger alarms. The following alarm events can be added: ● Brute-force attacks ● Abnormal logins
Add to alarm whitelist	Add false alarmed items to the login whitelist. HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms. After adding an alarm to the alarm whitelist, you can customize a whitelist rule. The custom rule types vary depending on the alarm types, including the file path, process path, process command line, remote IP address, and user name. If a detected alarm event hit the rule you specified, HSS does not generate an alarm. For details about events that can be isolated and killed, see **Server Alarms**.

Step 8 Click **OK**.

You check handled alarms. For details, see **Handling History**.

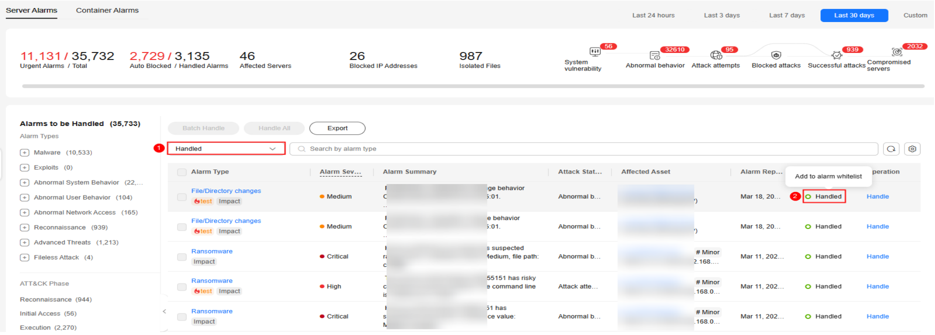
----End

Viewing the Handling History of an Alarm

Step 1 In the alarm event list, filter handled alarms.

Step 2 Hover the cursor over **Status** of an alarm to view its handling history.

Figure 8-6 Viewing the handling history of an alarm



Alarm Type	Alarm Sev...	Alarm Summary	Attack Stat...	Affected Asset	Alarm Rep...		peration
File/Directory changes test Impact	Medium	[redacted] ge behavior 5:01.	Abnormal b...	[redacted] ')	Mar 18, 20...	Handled	Handle
File/Directory changes test Impact	Medium	[redacted] e behavior 5:01.	Abnormal b...	[redacted] ')	Mar 18, 20...	Handled	Handle
Ransomware Impact	Critical	[redacted] s suspected Medium, file path:	Abnormal b...	[redacted] # Minor 2.168....	Mar 11, 202...	Handled	Handle
Ransomware test Impact	High	[redacted] 55151 has risky e command line	Attack atte...	[redacted] # Minor .168.0...	Mar 11, 202...	Handled	Handle
Ransomware Impact	Critical	[redacted] 51 has ce value:	Abnormal b...	[redacted] # Minor .168.0...	Mar 11, 202...	Handled	Handle

----End

Canceling Handled Server Alarms

You can cancel the processing of a handled alarm event.

Step 1 In the alarm event list, filter handled alarms.

Step 2 In the **Operation** column of an alarm, click **Handle**.

Step 3 In the **Handle Alarm Event** dialog box, click **OK** to cancel the last handling.

----End

8.1.4 Exporting Server Alarms

You can export server alarms and events to a local PC.

Exporting Server Alarms

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Detection & Response** > **Alarms**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Server Alarms** tab.

Step 6 Click **Export** above the alarm list to export all security events.

To export the alarms of a certain type or ATT&CK attack phase, select the type or phase in the **Alarms to Be Handled** area and click **Export**.

Step 7 View the export status in the upper part of the alarms page. After the export is successful, obtain the exported information from the default file download address on the local host.

NOTICE

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

8.1.5 Managing Isolated Files

HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** page. You can click **Isolated Files** on the upper right corner to check them, and can recover or delete isolated files anytime.

For details about events that can be isolated and killed, see **Server Alarms**.

Constraints

Servers that are not protected by HSS do not support alarm-related operations.

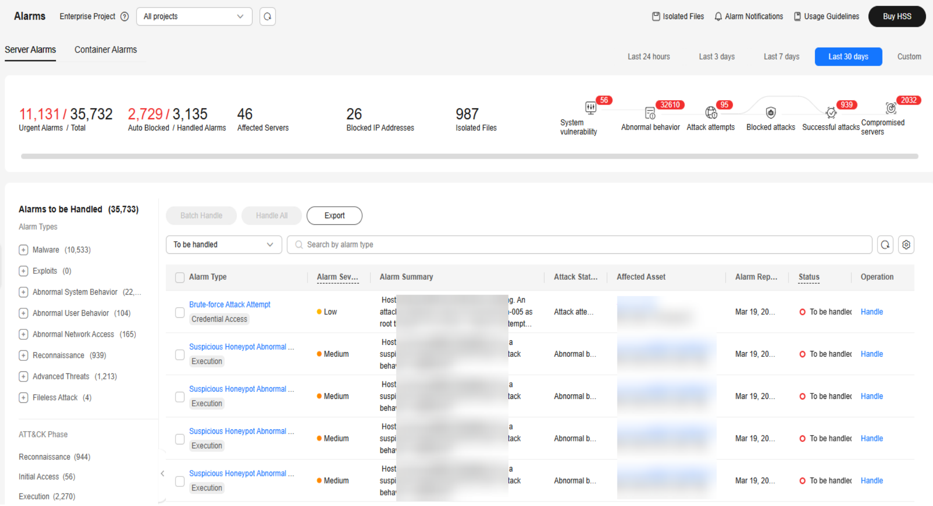
Isolation and Killing Operations

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

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

Step 3 In the navigation pane on the left, choose **Detection & Response** > **Alarms** and click **Server Alarms**.

Figure 8-7 Server alarms



☐ Alarm Type	Alarm Sev...	Alarm Summary	Attack Stat...	Affected Asset	Alarm Rep...	Status	Operation
☐ Brute-force Attack Attempt Credential Access	● Low	Host attacl [redacted] ıg. An -005 as root t [redacted] tempt...	Attack atte...	[redacted]	Mar 19, 20...	○ To be handlec	Handle
☐ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handlec	Handle
☐ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handlec	Handle
☐ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handlec	Handle
☐ Suspicious Honeypot Abnormal ... Execution	● Medium	Host suspi beha [redacted] a tack	Abnormal b...	[redacted]	Mar 19, 20...	○ To be handlec	Handle

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Locate an event that can be isolated and killed, click **Handle** in the **Operation** column, and select **Isolate and Kill** in the displayed box.

NOTE

For details about events that can be isolated and killed, see **Server Alarms**.

Step 6 Click **OK** and isolate and kill the target alarm event.

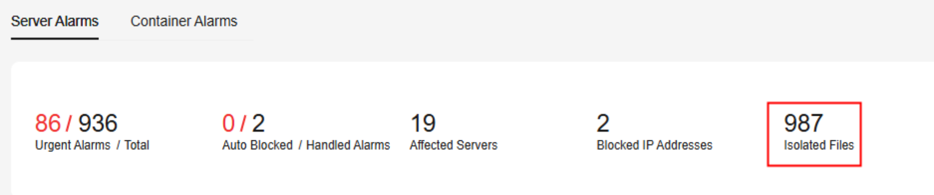
Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** page and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check them.

----End

Checking Isolated Files

Step 1 In the alarm statistics area on the **Server Alarms** page, click the number above **Isolated Files** to check the isolated files.

Figure 8-8 Alarm statistics



Step 2 Check the servers, names, paths, and modification time of the isolated files.

----End

Restoring Isolated Files

If you want to de-isolate an isolated file, you can restore it by referring to the following steps. The permissions for this file will be restored to what they were before it was isolated. Exercise caution when performing this operation.

Step 1 Click **Restore** in the **Operation** column of the list. The dialog box is displayed.

Step 2 Click **OK**.

----End

Deleting Isolated Files

If you want to permanently delete an isolated file, you can perform the deletion operation by referring to the following steps.

Step 1 Click **Delete** in the **Operation** column of the list. The dialog box is displayed.

To delete isolated files in batches, select multiple isolated files and click **Delete** in the upper left corner of the list.

Step 2 Click **OK**.

----End

8.2 Container Alarms

8.2.1 Container Alarm Events

After node protection is enabled, an agent is deployed on each container host to monitor the running status of containers in real time. The agents support escape detection, high-risk system calls, abnormal processes, abnormal files, and container environment detection. You can learn alarm events comprehensively on the **Container Alarms** page, and eliminate security risks in your assets in a timely manner.

Constraints

- Only the HSS container edition supports container security alarms. For details about how to purchase and upgrade HSS, see **Purchasing HSS** and **Upgrading Quota**.

Container Security Alarms

For details about container security alarm types and items, see **Table 8-7**.

Table 8-7 Container security alarms

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Malware	Malicious software includes viruses, worms, Trojans, and web shells implanted by hackers to steal your data or control your servers. For example, hackers will probably use your servers as miners or DDoS zombies. This occupies a large number of CPU and network resources, affecting service stability.	Unclassified malware	Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing.
		Viruses	Check containers in real time and report alarms for viruses detected in the container runtime.
		Worms	Detect worms in container runtime and report alarms.
		Trojans	Detect and remove Trojan and viruses in containers and report alarms.
		Botnets	Detect and kill botnets in containers and report alarms.
		Backdoors	Detect backdoors in containers and report alarms.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Rootkits	Check container assets and report alarms for suspicious kernel modules, files, and folders.
		Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.
		Web shells	Check whether the files (often PHP and JSP files) in the web directories on containers are web shells.
		Hacker tools	Report alarms on the malicious behaviors that exploit vulnerabilities or are performed using hacker tools.
		Mining software	Detect programs that are hidden in normal programs and have special functions such as damaging and deleting files, sending passwords, and recording keyboards. If a suspicious program is detected, an alarm is reported immediately.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Vulnerability Exploits	The exploit of vulnerabilities in the server system, software, or network to obtain unauthorized access rights, steal data, or damage the target system. Exploits can be performed remotely or locally. In a remote vulnerability exploit, an attacker connects to the target system through the network and discovers system vulnerabilities to launch attacks. In a local vulnerability exploit, an attacker obtains low access permissions on the target system and exploits vulnerabilities to escalate permissions or perform other malicious operations.	Vulnerability escapes	A vulnerability escape attack exploits application vulnerabilities, container infrastructure vulnerabilities, orchestration system vulnerabilities, or container runtime vulnerabilities to bypass the security mechanism and obtain unauthorized access permissions or perform unauthorized operations. HSS reports an alarm if it detects container process behavior that matches the behavior of known vulnerabilities (such as Dirty COW, brute-force attack, runC, and shocker).
		File escapes	In file escape attacks, attackers exploit file system or application vulnerabilities to bypass file permission restrictions and access or modify unauthorized files or directories. HSS reports an alarm if it detects that a container process accesses a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms. **NOTE** UOS 1050u2e does not support file escape detection.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Abnormal System Behaviors	Abnormal system behaviors occur while servers are running, and are usually caused by system faults, malicious attacks, or security vulnerabilities. Abnormal system behaviors may cause data loss or system breakdown. To protect server system and data security, it is important to detect and handle abnormal system behaviors in a timely manner.	Reverse shells	Monitor user process behaviors in real time to report alarms on and block reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. You can configure the reverse shell detection rule in the **Malicious File Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands. To enable automatic reverse shell blocking, enable **Auto Blocking** in the **HIPS Detection** policy on the **Policies** page. Currently, the following types of reverse shells can be blocked: exec reverse shell, Perl reverse shell, AWK reverse shell, Python reverse shell.b, Python reverse shell.a, Lua reverse shell, mkfifo/openssl reverse shell, PHP reverse shell, Ruby reverse shell, rssocks reverse proxy, Bash reverse shell, Ncat reverse shell, exec redirection reverse shell, Node reverse shell, Telnet dual-port reverse shell, nc reverse shell, Socat reverse shell, rm/mkfifo/sh/nc reverse shell, and socket/tchsh reverse shell. **NOTE** Before you enable auto blocking of reverse shells, ensure you have enabled the function of **isolating and killing malicious programs**.
		File privilege escalation	Report alarms on root privilege escalations exploiting SUID and SGID program vulnerabilities.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Process privilege escalations	After hackers intrude containers, they will try exploiting vulnerabilities to grant themselves the root permissions or add permissions for files. In this way, they can illegally create system accounts, modify account permissions, and tamper with files. HSS can detect the following abnormal privilege escalation operations: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities ● File privilege escalation
		Important file changes	Monitor important system files (such as ls, ps, login, and top) in real time and generate alarms if these files are modified. For more information, see **Monitored important file paths**. HSS reports all the changes on important files, regardless of whether the changes are performed manually or by processes.
		File/ Directory changes	Monitor system files and directories in real time and generate alarms if such files are created, deleted, moved, or if their attributes or content are modified.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: ● Abnormal process path: A process path containing abnormal marks, such as hidden, temporary, and file deletion records. Scored 1 to 3 points. ● Abnormal process connection: Access to malicious IP addresses. Scored 3 to 6 points. ● Process CPU exception: Abnormal CPU usage of a process. Scored 1 point. ● Abnormal executable file of a process: A process executable file containing abnormal characters. Scored 3 points. If the total score of abnormal processes is greater than or equal to 3, an alarm is reported, and the matched rules and their scores are displayed.
		High-risk system calls	Users can run tasks in kernels by Linux system calls. CGS reports an alarm if it detects a high-risk call, such as **open_by_handle_at**, **ptrace**, **setns**, and **reboot**.
		Abnormal shells	Check containers for actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. You can configure the abnormal shell detection rule in the **Malicious File Detection** rule on the **Policies** page. HSS will check for suspicious or remotely executed commands.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		High-risk command executions	Check executed commands in containers and generate alarms if high-risk commands are detected.
		Abnormal container processes	● Malicious container program HSS monitors container process behavior and process file fingerprints. It reports an alarm if it detects a process whose behavior characteristics match those of a predefined malicious program. ● Abnormal processes Container services are usually simple. If you are sure that only specific processes run in a container, you can whitelist the processes on the **Policy Groups** page, and associate the policy with the container. HSS reports an alarm if it detects that a process not in the whitelist is running in the container.
		Sensitive file access	HSS monitors the container image files associated with file protection policies, and reports an alarm if the files are modified.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Abnormal container startups	HSS monitors container startups and reports an alarm if it detects that a container with too many permissions is started. This alarm does not indicate an actual attack. Attacks exploiting this risk will trigger other HSS container alarms. HSS container check items include: ● Privileged container startup (**privileged:true**) Alarms are triggered by the containers started with the maximum permissions. Settings that can trigger such alarms include the **–privileged=true** parameter in the **docker run** command, and **privileged: true** in the **securityContext** of the container in a Kubernetes pod. If the alarm name is **Container Security Options** and the alarm content contains **privileged:true**, it indicates that the container is started in privileged container mode. ● Too many container capabilities (**capability:[xxx]**) In Linux OSs, system permissions are divided into groups before assigned to containers. A container only has a limited number of permissions, and the impact scope of this container is limited in the case of an incident. However, malicious users can grant all the system permissions to a container by modifying its startup configurations. If the alarm name is **Container Security Options** and the alarm content contains **capabilities: [xxx]**, it indicates that the container is started with an overlarge capability set, which poses risks. ● Seccomp not enabled (**seccomp=unconfined**)

Alarm Type	Alarm Type Description	Alarm	Alarm Description
			Secure computing mode (seccomp) is a Linux kernel feature. It can restrict system calls invoked by processes to reduce the attack surface of the kernel. If **seccomp=unconfined** is configured when a container is started, system calls will not be restricted for the container. If the alarm name is **Container Security Options** and the alarm content contains **seccomp=unconfined**, it indicates that the container is started without seccomp, which poses risks. **NOTE** If seccomp is enabled, permissions will be verified for every system call. The verifications will probably affect services if system calls are frequent. Before you decide whether to enable seccomp, you are advised to test-enable it and analyze the impact on your services. ● Container privilege escalation (**no-new-privileges:false**) Processes can escalate permissions by running the **sudo** command and using SUID or SGID bits. Default container configurations do not allow privilege escalation. If **–no-new-privileges=false** is specified when a container is started, the container can escalate privileges. If the alarm name is **Container Security Options** and the alarm content contains **no-new-privileges:false**, it indicates that privilege escalation restriction is disabled for the container, which poses risks. ● High-risk directory mapping (**mounts:[...]**) For convenience purposes, when a container is started on a

Alarm Type	Alarm Type Description	Alarm	Alarm Description
			server, the directories of the server can be mapped to the container. In this way, services in the container can directly read and write resources on the server. However, this mapping incurs security risks. If any critical directory in the server OS is mapped to the container, improper operations in the container will probably damage the server OS. HSS reports an alarm if it detects that a critical server path (**/boot**, **/dev**, **/etc**, **/sys**, and **/var/run**) is mounted during container startup. If the alarm name is **Container Mount Point** and the alarm content contains **mounts: [{"source":"xxx","destination": "yyy"...]**, it indicates that a file path mapped to the container is unsafe. In this case, check for risky directory mappings. You can configure the mount paths that are considered secure in the container information collection policy. **NOTE** Alarms will not be triggered for the files that need to be frequently accessed by Docker containers, such as **/etc/hosts** and **/etc/resolv.conf**. ● Startup of containers in the **host** namespace The namespace of a container must be isolated from that of a server. If a container and a server use the same namespace, the container can access and modify the content on the server, which incurs container escape risks. To prevent such problems, HSS checks the container PID, network, and whether the container namespace is **host**.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
			If the alarm name is **Container Namespace** and the alarm content contains **Container PID Namespace Mode**, **Container IPC Namespace Mode**, or **Container Network Namespace Mode**, it indicates that a container whose namespace is **host** is started. In this case, check the container startup options based on the alarm information. If you are sure that the container can be trusted, you can ignore the alarm.
		Container Image blocking	If a container contains insecure images specified in the **Suspicious Image Behaviors**, before the container is started, an alarm will be generated for the insecure images. **NOTE** You need to **install the Docker plug-in**.
		Suspicious command executions	● Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. ● Detect suspicious remote command execution.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Abnormal runtime behaviors	Abnormal runtime behaviors refer to suspicious behaviors that occur during container running. These behaviors may affect container security or even be exploited by attackers to escape containers. HSS can detect container escapes at the levels of networks, servers, pods, containers, processes, and system calls. Five types of abnormal behaviors (processes, files, network activities, process capabilities, and system calls) in containers and their hosts can be detected, reported, and blocked to prevent container escape and protect container runtime. ● Process monitoring: Monitor suspicious process behaviors in containers and their hosts, and detect and prevent abnormal system calls and process operations, for example, using **cdk evaluate** to collect container information through container penetration test tools. ● File system monitoring: Monitor file system operations in containers and their hosts, and detect and prevent unauthorized file access and modification, for example, running the **echo "test" /etc/profile** command to modify key system files. ● Network activity monitoring: Monitor network activities in containers and their hosts, and detect and prevent abnormal network connections and data transmission, for example, running the **wget 127.0.0.x** command to connect to the destination IP address in a container. ● Process capabilities monitoring: Monitor the capabilities of processes in containers and their

Alarm Type	Alarm Type Description	Alarm	Alarm Description
			hosts, and detect and prevent suspicious capability configuration, for example, running the **mknod -m 640 /tmp/test4 c 100 2** command to mount the devices represented by special strings. ● System call monitoring: Monitor system calls in the containers and their hosts, and detect and prevent high-risk system calls, for example, running the **chown root.root /opt/testfile** command to change the owner and owner group of files in a container. Containers that meet the following conditions can be scanned for abnormal runtime behaviors: ● The Linux kernel version is 5.10 or later. ● BPF LSM is enabled. To use abnormal runtime behavior detection, configure and enable the container escape prevention policy. For details, see **Configuring Policies**.
Abnormal User Behavior	Abnormal or unexpected user behaviors that occur in a specific environment or system, sometimes within a short period of time, such as abnormal logins or unauthorized access. To detect and identify these abnormal behaviors, user operations need to be checked and analyzed.	Invalid accounts	Hackers can probably crack unsafe accounts on your containers and control the containers. HSS checks suspicious hidden accounts and cloned accounts and generates alarms on them.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Brute-force attacks	Detect and report alarms for brute-force attack behaviors, such as brute-force attack attempts and successful brute-force attacks, on containers. Detect SSH, web, and Enumdb brute-force attacks on containers. **NOTE** ● Currently, brute-force attacks can be detected only in the Docker runtime. ● Ubuntu 24.04 and SUSE 15 SP6 do not support brute-force attack detection.
		Password thefts	Report alarms on user key theft.
Abnormal Network Access	Abnormal network access refers to exceptions that occur during network connection or data transmission and different from normal usage. These exceptions include abnormal resource usage, unauthorized access, and abnormal connections. Abnormal network access behaviors on servers may be a prelude to attacks.	Abnormal outbound connections	Report alarms on suspicious IP addresses that initiate outbound connections from containers. Only the containers with kernel 5.10 or later can be checked.
		Port forwarding	Report alarms on port forwarding using suspicious tools.
Abnormal Cluster Behaviors	Abnormal cluster behaviors occur in the cluster environment, such as pod creation, execution exceptions, and user information enumeration. These exceptions may indicate that the cluster is under an attack.	Abnormal pod behaviors	Detect abnormal operations such as creating privileged pods, static pods, and sensitive pods in a cluster and abnormal operations performed on existing pods and report alarms.
		User information enumerations	Detect the operations of enumerating the permissions and executable operation list of cluster users and report alarms.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
		Binding cluster roles	Detect operations such as binding or creating a high-privilege cluster role or service account and report alarms.
		Kubernetes event deletions	Detect the deletion of Kubernetes events and report alarms.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
Fileless Attacks	A fileless attack does not release malicious executable files. Instead, it writes malicious code into the system memory or registry. Because there are no malicious files used, such an attack is difficult to detect. Fileless attacks are classified into the following types based on disk file activities: ● No file activities. That is, no disk files are stored or operated in disks. Generally, such attacks are initiated in the upper-layer hardware, firmware, or software layer rather than the OS. ● Indirect activities through files. That is, no files are stored in disks, but activities are indirectly performed through files. Malicious code is usually indirectly loaded to the memory for execution through white files. Most of such malicious code is carried by scripts, which are executed through	Process injection	Scan for malicious code injection into running processes and report alarms.
		Dynamic library injection	Scan for the payloads injected by hijacking functions in the dynamic link library (DLL) and report alarms.
		Memory file process	Scan for the behaviors of creating an anonymous malicious file that exists only in the RAM through the memfd_create system call and executing the file, and report alarms on such behaviors.

Alarm Type	Alarm Type Description	Alarm	Alarm Description
	program commands or specific mechanisms such as disk boot records. ● File activities required. Generally, malicious code is converted into data. Attackers exploit file-related program vulnerabilities or features to convert malicious data into malicious code for execution.		

Security Alarm Severities

HSS alarm severities indicate alarm impact on service systems. It can be Critical, High, Medium, or Low. For details, see **Table 8-8**.

Table 8-8 Security alarm severities

Alarm Severity	Description
Critical	A critical alarm indicates that the system is severely attacked, which may cause data loss, system breakdown, or long service interruption. For example, such alarms are generated if ransomware encryption behaviors or malicious programs are detected. You are advised to handle the alarms immediately to avoid severe system damage.
High	A high-risk alarm indicates that the system may be under an attack that has not caused serious damage. For example, such alarms are generated if unauthorized login attempts are detected or unsafe commands (for deleting critical system files or modifying system settings) are executed. You are advised to investigate and take measures in a timely manner to prevent attacks from spreading.

Alarm Severity	Description
Medium	A medium-risk alarm indicates that the system has potential security threats, but there are no obvious signs of being attacked. For example, if abnormal modifications of a file or directory are detected, there may be potential attack paths or configuration errors in the system. You are advised to further analyze and take proper preventive measures to enhance system security.
Low	A low-risk alarm indicates that a minor security threat exists in the system but does not have significant impact on your system. For example, such alarms are generated if port scans are detected, indicating that there may be attackers trying to find system vulnerabilities. These alarms do not require immediate emergency measures. If you have high requirements on asset security, pay attention to the security alarms of this level.

Monitored important file paths

Type	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

8.2.2 Viewing Container Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of urgent alarms, total alarms, containers with alarms, and handled alarms.

The **Events** page displays the alarm events generated in the last 30 days.

The status of a handled event changes from **Unhandled** to **Handled**.

Constraints

Servers that are not protected by HSS do not support operations related to alarms and events.

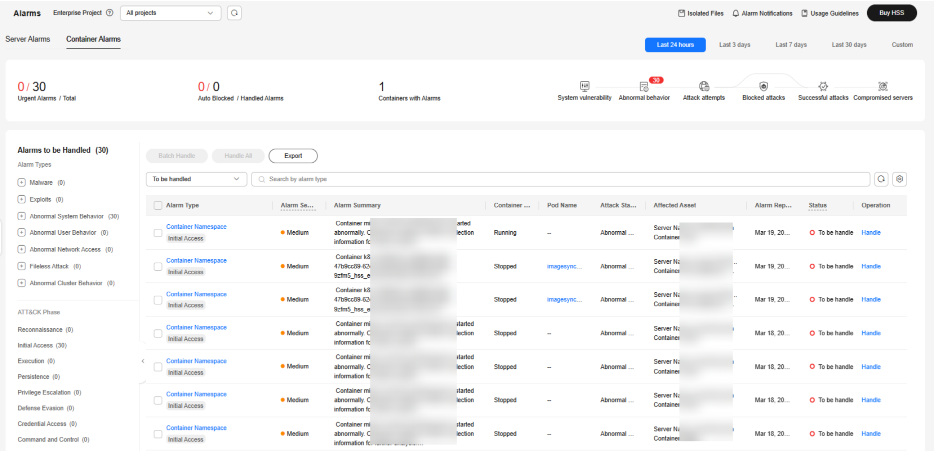
Viewing Container Alarms

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Detection & Response** > **Alarms** and click the **Container Alarms** tab to view container alarms and events.

Figure 8-9 Container alarms



0 / 30
Urgent Alarms / Total

0 / 0
Auto Blocked / Handled Alarms

1
Containers with Alarms

Alarms to be Handled (30)

Alarm Types
- Malware (0)
- Exploits (0)
- Abnormal System Behavior (30)
- Abnormal User Behavior (0)
- Abnormal Network Access (0)
- Fileless Attack (0)
- Abnormal Cluster Behavior (0)

ATT&CK Phase
- Reconnaissance (0)
- Initial Access (30)
- Execution (0)
- Persistence (0)
- Privilege Escalation (0)
- Defense Evasion (0)
- Credential Access (0)
- Command and Control (0)

Alarm Type	Alarm Se...	Alarm Summary	Container ...	Pod Name	Attack Sta...	Affected Asset	Alarm Rep...	Status	Operation
Container Namespace Initial Access	Medium	Container mi [redacted] arted abnormally. C [redacted] lection information fc	Running	--	Abnormal ...	Server Na [redacted] Container	Mar 19, 20...	To be handle	Handle
Container Namespace Initial Access	Medium	Container k8 [redacted] 47b9cc89-62 [redacted] 9zfm5_hss_e	Stopped	imagesync...	Abnormal ...	Server Na [redacted] Container	Mar 19, 20...	To be handle	Handle
Container Namespace Initial Access	Medium	Container k8 [redacted] 47b9cc89-62 [redacted] 9zfm5_hss_e	Stopped	imagesync...	Abnormal ...	Server Na [redacted] Container	Mar 19, 20...	To be handle	Handle
Container Namespace Initial Access	Medium	Container mi [redacted] started abnormally. C [redacted] lection information fc	Stopped	--	Abnormal ...	Server Na [redacted] Container	Mar 18, 20...	To be handle	Handle
Container Namespace Initial Access	Medium	Container mi [redacted] started abnormally. C [redacted] lection information fc	Stopped	--	Abnormal ...	Server Na [redacted] Container	Mar 18, 20...	To be handle	Handle
Container Namespace Initial Access	Medium	Container mi [redacted] started abnormally. C [redacted] lection information fc	Stopped	--	Abnormal ...	Server Na [redacted] Container	Mar 18, 20...	To be handle	Handle
Container Namespace Initial Access	Medium	Container mi [redacted] started abnormally. C [redacted] lection information fc [redacted]	Stopped	--	Abnormal ...	Server Na [redacted] Container	Mar 18, 20...	To be handle	Handle

Table 8-9 Container alarm statistics

Parameter	Description
Urgent Alarms / Total	Number of alarms to be handled and total number of alarms. You can click a number to view the alarm list.
Auto Blocked / Handled Alarms	Number of blocked alarms and number of handled alarms. Click a number to view the alarm list.
Containers with Alarms	Number of containers for which alarms are generated.

- **Viewing the alarms of a certain type or ATT&CK phase**

  In the **Alarms to Be Handled** area, select an alarm type or att&ck phase. For details, see ATT&CK attack phase description.

  NOTE

  Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a framework that helps organizations understand the cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle.

Table 8-10 ATT&CK phases

ATT&CK Phase	Description
Reconnaissance	Attackers seek vulnerabilities in your system or network.
Initial Access	Attacker try to enter your system or network.
Execution	Attackers try to run malicious code.
Persistence	Attackers try to maintain their foothold.
Privilege Escalation	Attackers try to obtain higher permissions.
Defense Evasion	Attackers try to avoid being detected.
Credential Access	Attackers try to steal account names and passwords.
Command and Control	Attackers try to communicate with compromised machines to control them.
Impact	Attackers try to manipulate, interrupt, or destroy your system or data.

- **Viewing details about container alarms and events**

  Click an alarm name to go to its details page. You can view the alarm description, handling suggestion, alarm path and address in HSS forensics, and the handling history of similar alarms. **Table 8-11** describes the details of alarm information.

  NOTE

  For some HSS alarms that have been determined as malware alarms, the alarm source files are saved in the cloud center and you can download them. You can download the alarm source files to your local PC for analysis. The password for decompressing the files is **unlock**.

  For unacknowledged malware alarms, alarm source files cannot be downloaded. Check the actual service conditions and determine whether the files are malicious files.

Table 8-11 Alarm detail parameters

Parameter	Description
Intelligence Engine	Detection engines used by HSS, including the virus detection engine, AI detection engine, and malicious intelligence detection engine.
Attack Status	Status of the current threat.
First Occurred	Time when an attack alarm was first generated
Alarm ID	Unique ID of an alarm

Parameter	Description
ATT&CK Phase	For details about the attack technology models used by attackers in each phase, see **Table 8-10**.
Last Occurred	Time when an attack alarm was last generated
Alarm Information	Detailed information about an alarm, including the alarm description, alarm summary, affected assets, and handling suggestions.

Parameter	Description
Forensics	HSS investigates information such as the attack triggering path or virus type based on the alarm type, helping you quickly trace and locate the attack source. – **Process Tree**: If an alarm event contains process information, you can check the process ID, process file path, process command line, process startup time, and process file hash on the **Forensics** tab page. You can locate malicious processes based on such information. – **File Forensics**: If an alarm event contains file information, the file forensics information is displayed on the **Forensics** tab page. File forensics information includes the file path, file hash, file operation type, and user information (which may not be obtained for instantaneous processes). You can locate a file change based on the information. – Network Forensics: If an alarm event contains network-related information, you can check the local IP address, local port, remote IP address, remote port, and protocol on the **Forensics** tab. You can determine whether a user is unauthorized based on such information. – User Forensics: If an alarm event contains user-related information, you can check the user name, login IP address, login service type, login service port, last login event, and number of login failures on the **Forensics** tab. You can determine whether the access is unauthorized based on such information. – **Registry Forensics**: If an alarm event contains registry information, you can check the registry keys and values on the **Forensics** tab page. You can locate registry risks based on such information. – **Abnormal Login Forensics**: If an alarm event contains abnormal login information, you can check the login IP address and port number on the **Forensics** tab page. You can determine whether the login is trusted based on such information. – **Malware Forensics**: If an alarm event contains malware information, you can check the malware family, virus name, virus type, and confidence level on the **Forensics** tab page. – **Auto-started Item Forensics**: If an alarm event contains self-startup item information, you can check the user, command, self-startup item information, and process file command line information on the **Forensics** tab page. You can locate the auto-started items based on such information. – **Kernel Forensics**: If an alarm event contains kernel information, you can check system functions and kernel functions on the **Forensics** tab page. You can locate kernel risks based on the information.

Parameter	Description
	– **Container Forensics**: If an alarm event contains container information, you can check the container name and image ID on the **Forensics** tab page. You can locate container risks based on such information.
Similar Alarms	Alarm whose server and event type are the same as those of this alarm. You can handle the alarm according to the handling method of the similar alarms.

- **Viewing the pod details of a container alarm event**

  Click the pod name of the target alarm event to view the pod details, including the node IP address, namespace, pod IP address, pod label, and container list.

----End

8.2.3 Handling Container Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of urgent alarms, total alarms, containers with alarms, and handled alarms.

The **Events** page displays the alarms generated in the last 30 days.

The status of a handled alarm changes from **Unhandled** to **Handled**.

Constraints

Servers that are not protected by HSS do not support operations related to alarms and events.

Handling Container Alarms

This section describes how you should handle alarms to enhance server security.

NOTE

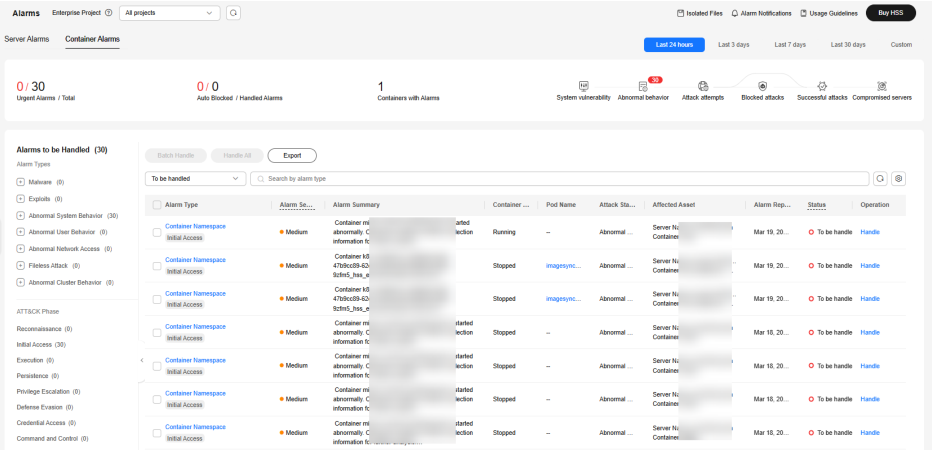
Do not fully rely on alarm handling to defend against attacks, because not every issue can be detected in a timely manner. You are advised to take more measures to prevent threats, such as checking for and fixing vulnerabilities and unsafe settings.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Detection & Response** > **Alarms**, and click **Container Alarms**.

Figure 8-10 Container alarms



☐	Alarm Type	Alarm Se...	Alarm Summary	Container ...	Pod Name	Attack Sta...	Affected Asset	Alarm Rep...	Status	Operation
☐	Container Namespace Initial Access	● Medium	Container mi [redacted] arted abnormally. C lection information fc	Running	--	Abnormal ...	Server Na Container [redacted]	Mar 19, 20...	○ To be handle	Handle
☐	Container Namespace Initial Access	● Medium	Container k8 [redacted] 47b9cc89-62 9zfm5_hss_e	Stopped	imagesync...	Abnormal ...	Server Na Container [redacted]	Mar 19, 20...	○ To be handle	Handle
☐	Container Namespace Initial Access	● Medium	Container k8 [redacted] 47b9cc89-62 9zfm5_hss_e	Stopped	imagesync...	Abnormal ...	Server Na Container [redacted]	Mar 19, 20...	○ To be handle	Handle
☐	Container Namespace Initial Access	● Medium	Container mi [redacted] started abnormally. C lection information fc	Stopped	--	Abnormal ...	Server Na Container [redacted]	Mar 18, 20...	○ To be handle	Handle
☐	Container Namespace Initial Access	● Medium	Container mi [redacted] started abnormally. C lection information fc	Stopped	--	Abnormal ...	Server Na Container [redacted]	Mar 18, 20...	○ To be handle	Handle
☐	Container Namespace Initial Access	● Medium	Container mi [redacted] started abnormally. C lection information fc	Stopped	--	Abnormal ...	Server Na Container [redacted]	Mar 18, 20...	○ To be handle	Handle
☐	Container Namespace Initial Access	● Medium	Container mi [redacted] started abnormally. C lection information fc	Stopped	--	Abnormal ...	Server Na Container [redacted]	Mar 18, 20...	○ To be handle	Handle

Step 4 Click an alarm name to view the alarm details and suggestions.

Step 5 Handle alarms.

Check and handle alarms as needed. The status of a handled alarm changes from **Unhandled** to **Handled**.

- Handling a single alarm

  In the **Operation** column of an alarm, click **Handle**.

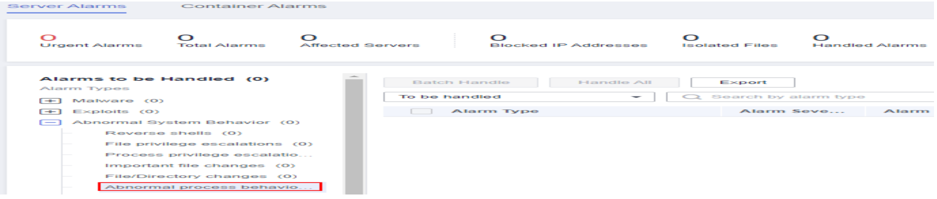
- Handling alarms in batches

  Select all alarms and click **Batch Handle** above the alarm list.

- Handling all alarms

  In the **Alarms to be Handled** area on the left pane of the alarm list, select an alarm type and click **Handle All** above the alarm list.

Figure 8-11 Handling all alarms



Step 6 In the **Handle Event** dialog box, select an action. For details about the processing modes, see Table 8-12.

When handling a single alarm event or handling alarms in batches, you can select **Handle duplicate alarms in batches** in the **Handle Event** dialog box.

Table 8-12 Alarm handling methods

Action	Description
Ignore	Ignore the current alarm. Any new alarms of the same type will still be reported by HSS.

Action	Description
Mark as handled	If you have manually handled an event, choose **Mark as handled**. You can add remarks to record details about event handling.
Add to Login Whitelist	Add false alarmed items of the **Brute-force attack** and **Abnormal login** types to the Login Whitelist. HSS will no longer report alarm on the Login Whitelist. A whitelisted login event will not trigger alarms. If the login IP address has been blocked, adding the login alarm event to the Login Whitelist will unblock the login IP address. The following alarm events can be added: ● Brute-force attacks ● Abnormal logins
Add to process whitelist	If you can confirm that a process triggering an alarm can be trusted, you can add it to the process whitelist.
Add to alarm whitelist	Add false alarmed items to the login whitelist. HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms. After adding an alarm to the alarm whitelist, you can customize a whitelist rule. The custom rule types vary depending on the alarm types, including the file path, process path, process command line, remote IP address, and user name. If a detected alarm event hit the rule you specified, HSS does not generate an alarm. For details about events that can be isolated and killed, see **Container Alarm Events**.

Step 7 Click **OK**.

You check handled alarms. For details, see **Historical Records**.

----End

Canceling Handled Container Alarms

You can cancel the processing of a handled alarm event.

Step 1 In the alarm event list, filter handled alarms.

Step 2 In the **Operation** column of an alarm, click **Handle**.

Step 3 In the **Handle Alarm Event** dialog box, click **OK** to cancel the last handling.

----End

8.2.4 Exporting Container Alarms

You can export container alarms and events to a local PC.

Exporting Container Alarms

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Detection & Response** > **Alarms**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Container Alarms** tab.

Step 6 Click **Export** above the alarm list to export all security events.

To export the alarms of a certain type or ATT&CK attack phase, select the type or phase in the **Alarms to Be Handled** area and click **to export**.

Step 7 View the export status in the upper part of the alarms page. After the export is successful, obtain the exported information from the default file download address on the local host.

Do not close the browser page during the export. Otherwise, the export task will be interrupted.

----End

8.3 Whitelist Management

8.3.1 Managing the Login Whitelist

You can configure the IP addresses of destination servers, login IP addresses, login usernames, and user behaviors on the **Login Whitelist** tab page.

You can:

- Add the false alarms of the **Brute-force attack** and **Abnormal login** types to the whitelist. For details, see **Viewing Server Alarms**.
- Add whitelist items on the **Login Whitelist** tab page.

Constraints

- If the destination server IP address, login IP address, and username of a login are all whitelisted, this login will be allowed without checking.
- To unblock IP addresses, add the IP address to the whitelist of the login security detection policy. For details, see **Login Security Check**.

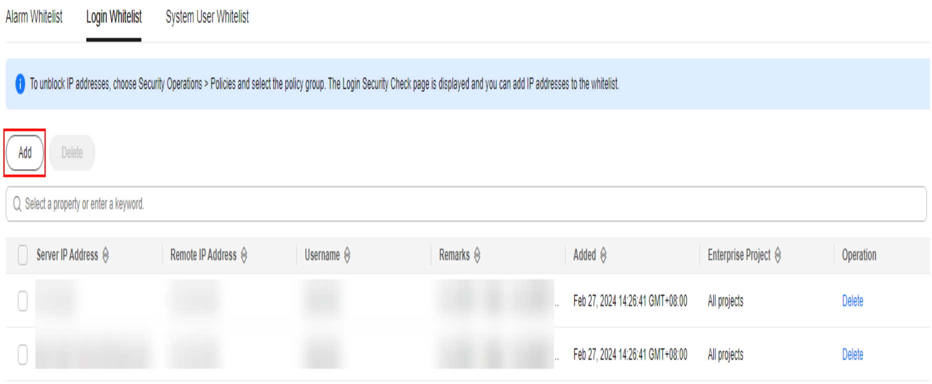
Adding Login Whitelist

Step 1 Log in to the management console.

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

Step 3 Choose **Detection & Response** > **Whitelists**. Click **Login Whitelist** and click **Add**.

Figure 8-12 Adding Login Whitelist



To unblock IP addresses, choose Security Operations > Policies and select the policy group. The Login Security Check page is displayed and you can add IP addresses to the whitelist.

Server IP Address	Remote IP Address	Username	Remarks	Added	Enterprise Project	Operation
[redacted]	[redacted]	[redacted]	[redacted]	Feb 27, 2024 14:26:41 GMT+08:00	All projects	Delete
[redacted]	[redacted]	[redacted]	[redacted]	Feb 27, 2024 14:26:41 GMT+08:00	All projects	Delete

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 On the displayed page, enter the server IP address, login IP address, and login username.

Table 8-13 Login Whitelist parameters

Parameter	Description	Example Value
Server IP Address	IP address or subnet mask of the destination server. ● IP address: for example, **192.168.1.1** or **16A0::1** ● IP subnet mask: for example, **192.168.7.0/24** or **16A0:10:AB00:1E::/64**	192.168.1.1
Login IP Address		
Login Username	Current login username	hss_test
Remarks	Custom whitelist description	Test
Handle historical alarms	After this option is selected, login alarms that have been generated will be synchronized.	Selected

Step 6 Click **OK**.

----End

Removing an Item from the Login Whitelist

Exercise caution when performing this operation. Whitelisted login alarms cannot be restored after removal, and will be reported once triggered. Up to 1000 alarm whitelist items can be deleted under an account.

- **Delete a login whitelist item**
  a. In the **Operation** column a server, click **Delete**.
  b. On the **Delete Whitelisted Login Item** page, confirm the information to be deleted, enter **DELETE**, and click **OK**.
  c. Return to the login alarm whitelist. Verify that the deleted login whitelist item is not displayed in the list.
- **Delete multiple login whitelist items**
  a. Select whitelist items and click **Delete** above the list.
  b. On the **Delete Login Alarm Whitelist** page, confirm the information to be deleted, enter **DELETE**, and click **OK**.
  c. Return to the login alarm whitelist. Verify that the deleted login whitelist item is not displayed.
- **Delete all login whitelist items**
  a. Click **Delete** above the login whitelist.
  b. In the **Delete All** dialog box, confirm the information to be deleted, enter **DELETE**, and click **OK**.
  c. Return to the login alarm whitelist. Verify that the deleted login whitelist item is not displayed.

8.3.2 Managing the Alarm Whitelist

You can configure the alarm whitelist to reduce false alarms. Events can be deleted from the whitelist.

Whitelisted events will not trigger alarms.

On the **Alarms** page, you can add falsely reported alarms to the alarm whitelist. After an alarm is added to the whitelist, HSS will not generate alarms on it.

Adding Events to the Alarm Whitelist

When handling an alarm event, you can select **Add it to alarm whitelist**. For details, see **Handling Server Alarms**.

Checking the Alarm Whitelist

Perform the following steps to check the alarm whitelist:

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

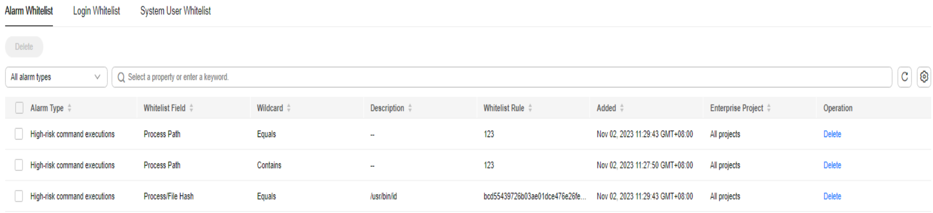
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Detection & Response** > **Whitelists**.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Alarm Whitelist** tab to view the whitelist. For more information, see **Table 8-14**.

Figure 8-13 Alarm whitelist



Alarm Type	Whitelist Field	Wildcard	Description	Whitelist Rule	Added	Enterprise Project	Operation
High-risk command executions	Process Path	Equals	--	123	Nov 02, 2023 11:29:43 GMT+08:00	All projects	Delete
High-risk command executions	Process Path	Contains	--	123	Nov 02, 2023 11:27:50 GMT+08:00	All projects	Delete
High-risk command executions	Process/File Hash	Equals	/usr/bin/id	bcd55439726b03ae01dce476e26fe...	Nov 02, 2023 11:29:43 GMT+08:00	All projects	Delete

Table 8-14 Alarm whitelist parameters

Parameter Name	Description
Alarm Type	Name of the alarm whitelist type.
Whitelist Field	Whitelisted file field
Wildcard	Logic used by a whitelisted rule, which can be equal or include.
Description	Description of the whitelist.
Whitelist Rule	Whitelisted rule ID
Added	Time when an alarm is added to the whitelist.
Enterprise Project	Enterprise project
Occurrences Today	Number of times that alarm events meet the whitelist conditions today.
Total Occurrences	Total number of times that alarm events meet the whitelist conditions. By default, this parameter is not displayed.

----End

Removing an Alarm from the Whitelist

Exercise caution when performing this operation. Whitelisted alarms cannot be restored after removal, and will be reported once triggered. Up to 10,000 alarm whitelist items can be deleted under an account.

- **Delete a whitelist item**
  a. In the **Operation** column of the item, click **Delete**.
  b. On the **Delete Whitelisted Alarm** page, confirm the information to be deleted and determine whether to restore associated alarms.

     When adding an alarm to the whitelist, you can whitelist similar alarms. Likewise, when deleting the whitelisted alarm, you can choose whether to restore these similar alarms.
  c. Enter **DELETE** in the text box and click **OK**.
  d. Return to the alarm whitelist. Verify that the deleted login whitelist item is not displayed.

- **Delete multiple alarm whitelist items**
  a. Select whitelist items and click **Delete** above the list.
  b. On the **Delete Whitelisted Alarm** page, confirm the information to be deleted and determine whether to restore associated alarms.

     When adding an alarm to the whitelist, you can whitelist similar alarms. Likewise, when deleting the whitelisted alarm, you can choose whether to restore the similar alarms.
  c. Enter **DELETE** in the text box and click **OK**.
  d. Return to the alarm whitelist. Verify that the deleted login whitelist item is not displayed.
- **Delete all alarm whitelist items**
  a. Click **Delete** above the alarm whitelist.
  b. On the **Delete All** page, confirm the information to be deleted, and choose whether to restore associated alarms.
  c. Enter **DELETE** in the text box and click **OK**.
  d. Return to the alarm whitelist. Verify that the deleted login whitelist item is not displayed.

8.3.3 Managing the System User Whitelist

HSS generates risky account alarms when non-root users are added to the root user group. You can add the trusted non-root users to the system user whitelist. HSS does not generate risky account alarms for users in the system user whitelist.

Adding an Item to the System User Whitelist

Step 1 Log in to the management console.

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

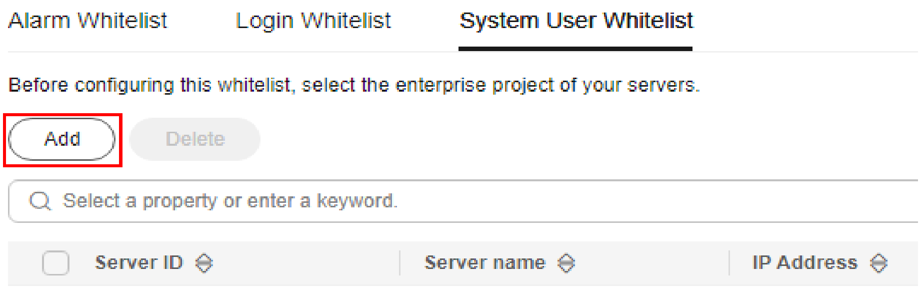
Step 3 In the navigation pane on the left, choose **Detection & Response** > **Whitelists**.

Step 4 (Optional) In the upper left corner of the **Whitelists** page, select the enterprise project to which the server belongs or **All projects** for **Enterprise Project**.

If you have not enabled the enterprise project function, skip this step.

Step 5 Click the **System User Whitelist** tab and click **Add**.

Figure 8-14 Configuring the system user whitelist



Before configuring this whitelist, select the enterprise project of your servers.

Step 6 In the **Add to System User Whitelist** dialog box, enter the server ID, system username, and remarks.

Step 7 Click **OK**.

----End

Modifying the System User Whitelist

Step 1 (Optional) In the upper left corner of the **Whitelists** page, select the enterprise project to which the server belongs or **All projects** for **Enterprise Project**.

If you have not enabled the enterprise project function, skip this step.

Step 2 In the row of the target system user whitelist, click **Modify** in the **Operation** column.

Step 3 In the **Modify System User Whitelist** dialog box, modify the information and click **OK**.

----End

Removing an Item from the System User Whitelist

After an account is deleted from the whitelist, HSS will report **Unsafe Accounts** alarms triggered by the account. Whitelisted items cannot be restored once deleted. Exercise caution when performing this operation. Up to 100 whitelisted system users can be deleted under an account.

Step 1 (Optional) In the upper left corner of the **Whitelists** page, select the enterprise project to which the server belongs or **All projects** for **Enterprise Project**.

If you have not enabled the enterprise project function, skip this step.

Step 2 In the **Operation** column of a whitelist item, click **Delete**.

To delete multiple whitelist items at a time, select them and click **Delete** above the list. To delete all the whitelist items, directly click **Delete**.

Step 3 In the displayed dialog box, confirm the information to be deleted, enter **DELETE**, and click **OK**.

Step 4 Return to the system user whitelist list. Verify that the deleted system users are not displayed.

----End

9 Security Operations

9.1 Policy Management

9.1.1 Policy Management Overview

What Is a Policy Group?

HSS comes in multiple editions, including basic, professional, enterprise, premium, WTP, and container editions. Except for the basic edition, they each have a default protection policy group. A policy group is a collection of policies. These policies can be applied to servers to centrally manage and configure the sensitivity, rules, and scope of HSS detection and protection.

You can create custom policy groups for HSS premium and container editions. If you have multiple servers protected by the premium or container edition but have different protection requirements for them, you can create custom policy groups for different servers and deploy different policy groups. For details, see **Creating a Custom Policy Group**.

What Policies Are Does a Policy Group Contain?

Policy groups vary by edition, as shown in **Table 9-1**. You can customize policies for asset management, baseline inspection, and intrusion detection as needed. For details, see **Configuring Policies**.

Table 9-1 Policies

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Asset management	Asset discovery	Scan and display all software in one place, including software name, path, and major applications, helping you identify abnormal assets.	Linux and Windows	Enabled	×	×	√	√	√
Baseline Inspection	Weak password detection	Change weak passwords to stronger ones based on HSS scan results and suggestions.	Linux and Windows	Enabled	√	√	√	√	√
	Configuration check	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.	Linux and Windows	Enabled	×	×	√	√	√
	Container information collection	Collect information about all containers on a server, including ports and directories, and report alarms for risky information.	Linux	Enabled	×	×	×	×	√

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Intrusion detection	Antivirus	Check server assets and report, isolate, and kill the detected viruses. The generated alarms are displayed under **Detection & Response** > **Alarms** > **Server Alarms** > **Event Types** > **Malware**. After antivirus is enabled, the resource usage is as follows: The CPU usage does not exceed 40% of a single vCPU. The actual CPU usage depends on the server status. For details, see **How Many CPU and Memory Resources Are Occupied by the Agent When It Performs Scans?**	Linux and Windows	Enabled	√	√	√	√	×
	Cluster intrusion detection	Detect container high-privilege changes, creation in key information, and virus intrusion.	Linux	Disabled	×	×	×	×	√

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Container escape	Check for and generate alarms on container escapes. If you do not want to detect container escape for certain containers, you can set the image, process, and pod name whitelist.	Linux	Disabled	×	×	×	×	√
	Container anti-escape	Container escape prevention can monitor abnormal runtime behaviors of five types (including processes, files, network activities, process capabilities, and system calls) on containers and their hosts; and report alarms and block abnormal behaviors to enhance container security. To use abnormal runtime behavior detection, configure a container escape prevention policy, select a protected object (a server or container), and enable the policy.	Linux	Disabled	×	×	×	×	√

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Container information module	You can configure a trusted container whitelist based on the container name, organization name to which the image belongs, and namespace. The container whitelist does not detect or generate alarms.	Linux	Enabled	×	×	×	×	√
	Webshell detection	Scan web directories on servers for web shells.	Linux and Windows	Enabled	√	√	√	√	√
	Container file monitoring	Detect file access that violates security policies. Security O&M personnel can check whether hackers are intruding and tampering with sensitive files.	Linux	Enabled	×	×	×	×	√
	Container process whitelist	Check for process startups that violate security policies.	Linux	Disabled	×	×	×	×	√
	Suspicious image behaviors	Configure the blacklist and whitelist and customize permissions to ignore abnormal behaviors or report alarms.	Linux	Disabled	×	×	×	×	√

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	HIPS detection	Check registries, files, and processes, and report alarms for operations such as abnormal changes.	Linux and Windows	Enabled	×	√	√	√	√
	File protection	Check the files in the Linux OS, applications, and other components to detect tampering.	Linux and Windows	Enabled	√	√	√	√	√

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Graph engine detection	Generally, threat behavior detection checks file, process, network, or other information against the threat feature library to identify and block malicious behaviors. But to identify an attack, which usually involves multiple steps, we need to correlate multiple behaviors. For example, a vulnerability exploit attack involves scan and reconnaissance, system intrusion, malicious file implant, and subsequent attacks. Graph engine detection performs comprehensive source tracing analysis based on the threat information provided by multiple modules (including HIPS detection, AI ransomware detection, and antivirus detection). It can associate and comprehensively analyze multiple suspicious process events to identify intrusion behaviors,	Windows	Enabled	×	×	√	√	√

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
		enhancing defense against vulnerability exploits.							

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Login security check	HSS can detect brute-force attacks on the following service accounts: ● Windows: RDP, SQL Server ● Linux: MySQL, vsftpd, SSH If five or more consecutive incorrect passwords are entered from the same IP address within 30 seconds, or the total number of incorrect passwords entered from the same IP address reaches 15 within 1 hour, HSS will generate an alarm for the latest user who entered an incorrect password from the IP address, and will block the IP address (for 12 hours by default) to prevent server intrusions caused by brute-force attacks. You can check whether a login IP address is trustworthy based on its attack type and how many times it has been blocked. You can manually unblock the IP addresses you trust.	Linux and Windows	Enabled	√	√	√	√	√

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Malicious file detection	● Reverse shell: Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. ● Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	Linux	Enabled	√	√	√	√	√
	External connection detection	Detect a process proactively connects to an external network.	Linux (kernel 5.10 or later)	Enabled	√	√	√	×	√
	Port scan detection	Detect scanning or sniffing on specified ports and report alarms.	Linux	Disabled	×	×	√	√	√

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Abnormal process behaviors	All the running processes on all your servers are monitored for you. You can create a process whitelist to ignore alarms on trusted processes, and can receive alarms on unauthorized process behavior and intrusions.	Linux	Enabled	√	√	√	√	√
	Root privilege escalation	Detect the root privilege escalation for files in the current system.	Linux	Enabled	√	√	√	√	√
	Real-time process	Monitor the executed commands in real time and generate alarms if high-risk commands are detected.	Linux and Windows	Enabled	√	√	√	√	√
	Rootkit detection	Detect server assets and report alarms for suspicious kernel modules, files, and folders.	Linux	Enabled	√	√	√	√	√
	Fileless attack detection	Scan for fileless attacks in user assets, including process injections, dynamic library injections, and memory file processes.	Linux	Disabled	×	×	√	√	√

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Self-protection	Windows self-protection	Prevent malicious programs from uninstalling the agent, tampering with HSS files, or stopping HSS processes.	Windows	Enabled	×	×	√	√	×

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
		NOTE ● Self-protection depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled. ● Enabling the self-protection policy has the following impacts: ● The agent cannot be uninstalled on the control panel of a server, but can be uninstalled on the HSS console. ● HSS processes cannot be terminated. ● In the agent installation path **C:\Program Files\HostGuard**, you can only access the **log** and **data** directories (and the **upgrade** directory, if your agent has been upgraded).							

Function Type	Policy	Description	Supported OS	Default Status	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	Linux self-protection	Prevent malicious programs from stopping the HSS process and uninstalling the agent. **NOTE** • Enabling the self-protection policy has the following impacts: • The agent cannot be uninstalled using commands but can be uninstalled on the HSS console. • HSS processes cannot be terminated.	Linux	Enabled	×	×	√	√	√

Policy Group Protection Modes

The Policy groups can detect threats in sensitive or balanced mode to meet the requirements of different scenarios. The two modes apply to the following scenarios:

- Sensitive mode: applicable to high security scenarios, such as network protection drills and key event security assurance. It achieves a high threat detection rate.
- Balanced mode: applicable to routine protection scenarios. The threat detection rate and accuracy are relatively balanced.

Policies affected by the protection mode: malicious file detection, web shell detection, HIPS detection, antivirus, and abnormal process behavior policies. For details about the differences between these policies in the two protection modes, see **Table 9-2**.

Table 9-2 Differences between policies in sensitive and balanced modes

Policy	Balanced Mode	Sensitive Mode
Malicious File Detection	● File size: 10 MB ● File types: ELF, Python, shell, and web shell	● File size: 50 MB ● File types: all
Web Shell Detection	The suspicious files that match YARA rules are not checked.	All files
HIPS Detection	Moderately sensitive	Highly sensitive. Compared with the balanced mode, it is more suitable for special detection rules in network protection drills and key event assurance.

Policy	Balanced Mode	Sensitive Mode
Antivirus	If **Protected File Type** is set to **All** for anti-virus detection, only the files with the following file name extensions are checked: ● **Linux** bat, bin, cmd, com, cpl, exe, gadget, inf1, ins, inx, isu, job, jse, js, lnk, msc, msi, msp, mst, paf, pif, ps1, reg, rgs, scr, sct, shb, shs, u3p, vb, vbe, vbs, vbscript, ws, wsf, wsh, doc, dot, wbk, docx, docm, dotm, docb, pdf, wll, wwl, xls, xlt, xlm, xll_, xla_, xla5, xla8, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xll, xlw, ppt, pot, pps, ppa, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, pa, accda, accdb, accde, accdt, accdr, accdu, mda, mde, one, ecf, pub, xps, png, tif, wmf, bmp, gif, jpeg, dwg, ico, pgp, psd, cdr, dxf, emf, eps, jp2, sgi, xpm, dll, sys, rar, zip, 7z, sh, cab, gz, gzip, xz, ace, tar, lzh, lha, bz, bz2, iso, jar, apk, jsp, jspx, php, asp, aspx, ashx, asmx, py, hta, ko ● **Windows** bat, bin, cmd, com, cpl, exe, gadget, inf1, ins, inx, isu, job, jse, js, lnk, msc, msi, msp, mst, paf, pif, ps1, reg, rgs, scr, sct, shb, shs, u3p, vb, vbe, vbs, vbscript, ws, wsf, wsh, doc, dot, wbk, docx, docm, dotm, docb, pdf, wll, wwl, xls, xlt, xlm, xll_, xla_, xla5, xla8, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xll, xlw, ppt, pot, pps, ppa, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, pa, accda, accdb, accde, accdt, accdr, accdu, mda, mde, one, ecf, pub, xps, png, tif, wmf, bmp, gif, jpeg, dwg, ico, pgp, psd, cdr, dxf, emf, eps, jp2, sgi, xpm, dll, sys, rar, zip, 7z, sh, cab, gz, gzip, xz, ace, tar, lzh, lha, bz, bz2, iso, jar, apk, jsp, jspx, php, asp, aspx, ashx, asmx, hta	If **Protected File Type** is set to **All** for anti-virus detection, all types of files are checked.

Policy	Balanced Mode	Sensitive Mode
Abnormal Process Behaviors	An alarm is generated only if multiple abnormal process behaviors are detected at the same time.	An alarm is generated immediately if an abnormal process behavior is detected.

9.1.2 Configuring Policies

Scenario

After HSS is enabled, you can configure HSS policies based on your service requirements.

Constraints

- The professional, enterprise, premium, WTP, or container edition is enabled.
- For the default policy groups, you are advised to retain their default configurations.
- Modifications on a policy take effect only in the group it belongs to.

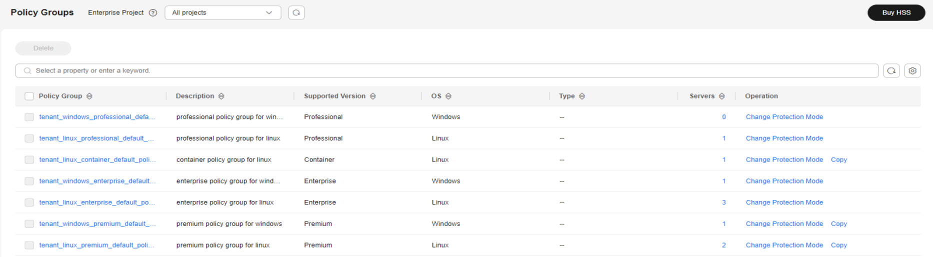
Accessing the Policies Page

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Security Operation** > **Policies**. On the displayed page, **Policy group parameters** describes the fields.

Figure 9-1 Policy management



Policy Group	Description	Supported Version	OS	Type	Servers	Operation
tenant_windows_professional_defa...	professional policy group for win...	Professional	Windows	--	0	Change Protection Mode
tenant_linux_professional_default_...	professional policy group for linux	Professional	Linux	--	1	Change Protection Mode
tenant_linux_container_default_poli...	container policy group for linux	Container	Linux	--	1	Change Protection Mode Copy
tenant_windows_enterprise_default...	enterprise policy group for wind...	Enterprise	Windows	--	1	Change Protection Mode
tenant_linux_enterprise_default_po...	enterprise policy group for linux	Enterprise	Linux	--	3	Change Protection Mode
tenant_windows_premium_default_...	premium policy group for windows	Premium	Windows	--	1	Change Protection Mode Copy
tenant_linux_premium_default_poli...	premium policy group for linux	Premium	Linux	--	2	Change Protection Mode Copy

Table 9-3 Policy group parameters

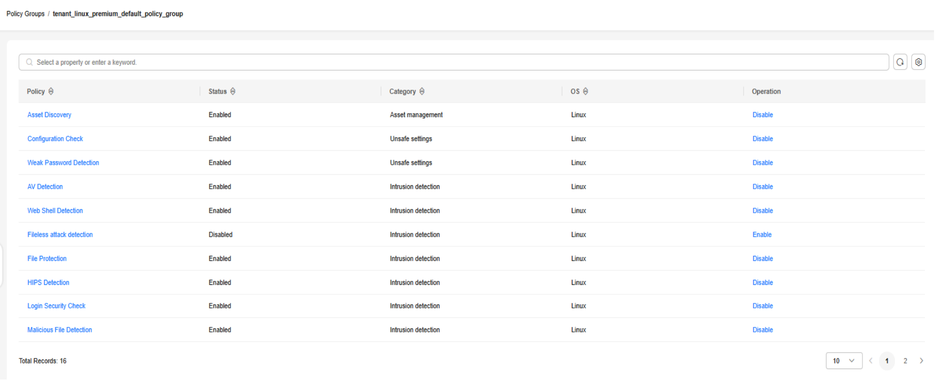
Parameter	Description
Policy Group	Name of a policy group The preset policy group names are as follows: ● **tenant_linux_advanced_default_policy_group**: preset policy of the Linux professional edition, which can only be viewed but cannot be copied or deleted. ● **tenant_windows_advanced_default_policy_group**: preset policy of the Windows professional edition, which can only be viewed but cannot be copied or deleted. ● **tenant_linux_container_default_policy_group**: preset Linux policy of the container edition. You can copy this policy group and create a new one based on it. ● **tenant_linux_enterprise_default_policy_group** is the default Linux policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. ● **tenant_windows_enterprise_default_policy_group**: preset Windows policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. ● **tenant_linux_premium_default_policy_group**: preset Linux policy of the premium edition. You can create a policy group by copying this default group and modify the copy. ● **tenant_windows_premium_default_policy_group**: preset Windows policy of the premium edition. You can create a policy group by copying this default group and modify the copy. ● **wtp_***ServerName* is a WTP edition policy group. It is generated by default when WTP is enabled for a server.
Description	Detailed description of a policy group.
Supported Version	HSS edition supported by a policy group.
Supported OS	OS supported by a policy group.
Associated Servers	To view details about the servers associated with a policy group, click the number in the **Servers** column of the group.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

- If **All projects** is selected, the policy change will apply to the servers under all enterprise projects.
- If a specific enterprise project is selected, the policy change will only apply to the servers under this project.

Step 5 Click the name of a policy group to access the policy detail list.

Figure 9-2 Policies



Policy Groups / tenant_linux_premium_default_policy_group

Policy	Status	Category	OS	Operation
Asset Discovery	Enabled	Asset management	Linux	Disable
Configuration Check	Enabled	Unsafe settings	Linux	Disable
Weak Password Detection	Enabled	Unsafe settings	Linux	Disable
AV Detection	Enabled	Intrusion detection	Linux	Disable
Web Shell Detection	Enabled	Intrusion detection	Linux	Disable
Fileless attack detection	Disabled	Intrusion detection	Linux	Enable
File Protection	Enabled	Intrusion detection	Linux	Disable
HIPS Detection	Enabled	Intrusion detection	Linux	Disable
Login Security Check	Enabled	Intrusion detection	Linux	Disable
Malicious File Detection	Enabled	Intrusion detection	Linux	Disable

Total Records: 16

Step 6 In the row of the policy, click **Enable** or **Disable** in the **Operation** column.

After a policy is disabled, HSS does not check for security issues based on the policy.

Step 7 Click the name of a policy to modify it. The following sections describe the policies.

----End

Asset Discovery

Step 1 Click **Asset Discovery**.

Step 2 On the displayed page, modify the settings as required. For more information, see **Table 9-4**.

Table 9-4 Parameter description

Parameter	Description
Scan Time	Fixed time for automatic assets scan. The scan time can be customized for middleware, web frameworks, kernel modules, web applications, websites, web services, and databases. Offset time is the automatic adjust ahead of or behind the specified scan time. ● Accounts: Linux accounts are automatically checked every hour, and Windows accounts are checked in real time. ● Open ports are automatically checked every 30 seconds. ● Processes are automatically checked every hour. ● Installed software is automatically checked once a day. ● Auto-started items are automatically checked every hour. ● Middleware/Web framework: You can select the scan date and time together. ● Kernel modules: You can set the scan date and time as required. ● Web applications/Websites/Web services/Databases: You can select the scan date and time together.
Scanned Web Directories	Specifies a web directory to be scanned.

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

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

----End

Weak Password Detection

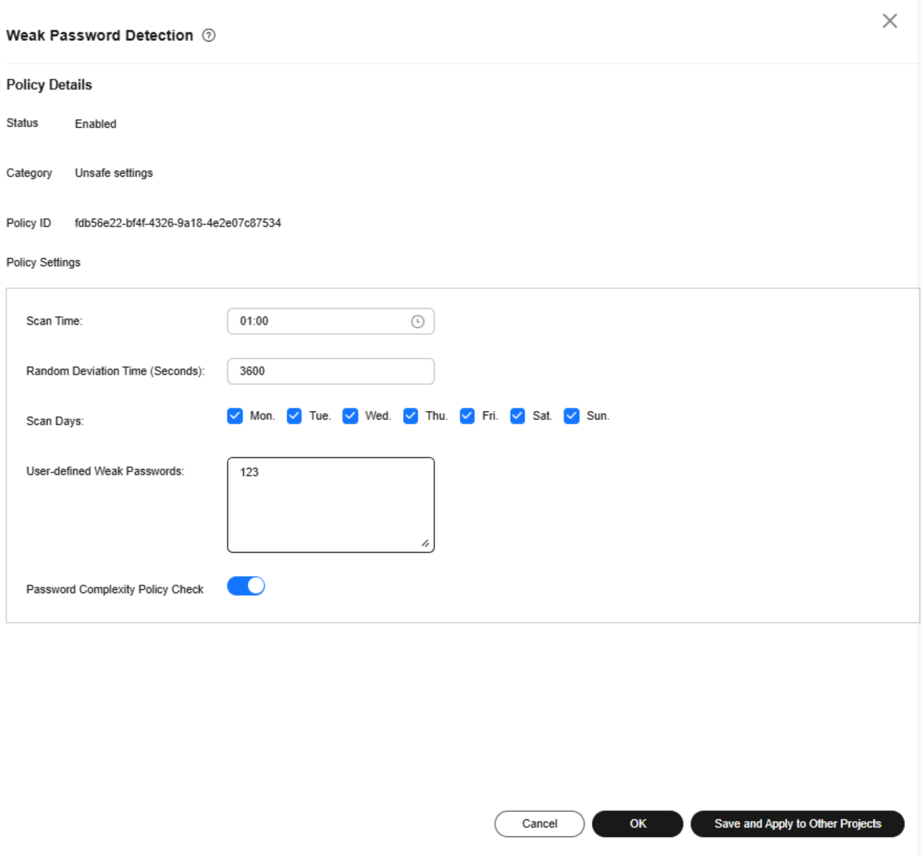
Weak passwords are not attributed to a certain type of vulnerabilities, but they bring no less security risks than any type of vulnerabilities. Data and programs will become insecure if their passwords are cracked.

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

Step 1 Click **Weak Password Detection**.

Step 2 In the **Policy Settings** area, modify the settings as required. For more information, see **Table 9-5**.

Figure 9-3 Modifying the weak password detection policy



Weak Password Detection ⓘ

Policy Details

Status Enabled

Category Unsafe settings

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

Policy Settings

Scan Time: 01:00

Random Deviation Time (Seconds): 3600

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

User-defined Weak Passwords: 123

Password Complexity Policy Check ●

Table 9-5 Parameter description

Parameter	Description
Scan Time	Time when scans are performed. It can be accurate to the minute.
Random Deviation Time (Seconds)	Random deviation time of the weak password based on **Scan Time**. The value range is 0 to 7,200s.
Scan Days	Days in a week when weak passwords are scanned. You can select one or multiple days.
User-defined Weak Passwords	You can add a password that may have been leaked to this weak password text box to prevent server accounts from using the password. Enter only one weak password per line. Up to 300 weak passwords can be added.
Password Complexity Policy Check	A password complexity policy refers to the password rules and standards set on a server. If you enable **Password Complexity Policy Check**, HSS will check the password complexity policy when you manually perform a baseline check.

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

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

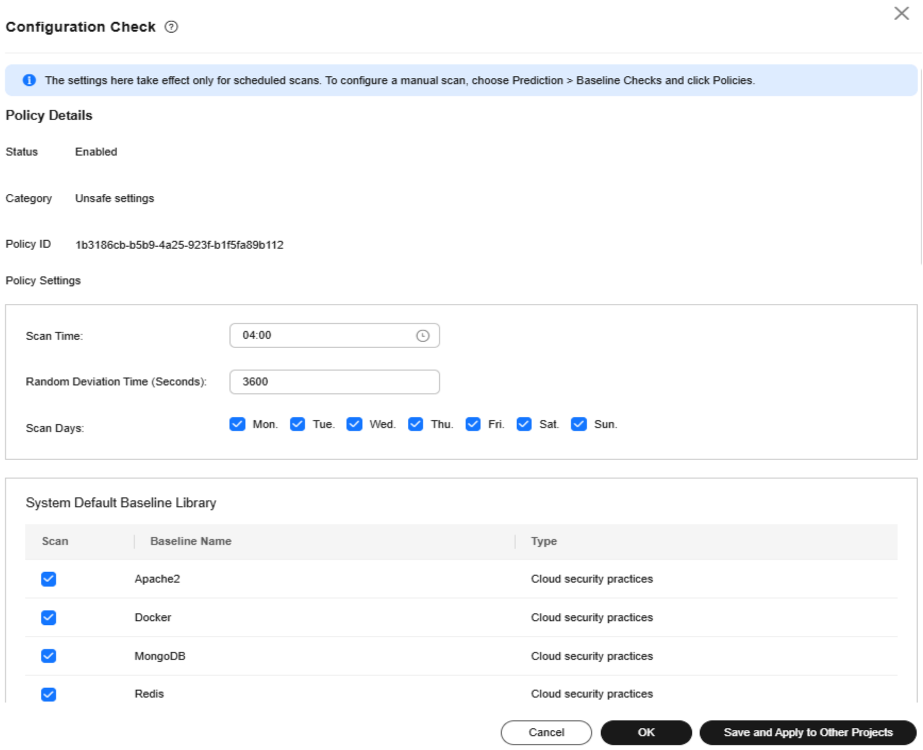
----End

Configuration Check

Step 1 Click **Configuration Check**.

Step 2 On the **Configure Check**, modify the policy.

Figure 9-4 Modifying the configuration check policy



Configuration Check ⓘ

ℹ The settings here take effect only for scheduled scans. To configure a manual scan, choose Prediction > Baseline Checks and click Policies.

Policy Details

Status Enabled

Category Unsafe settings

Policy ID 1b3186cb-b5b9-4a25-923f-b1f5fa89b112

Policy Settings

Scan Time: 04:00

Random Deviation Time (Seconds): 3600

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

System Default Baseline Library

Scan	Baseline Name	Type
☑	Apache2	Cloud security practices
☑	Docker	Cloud security practices
☑	MongoDB	Cloud security practices
☑	Redis	Cloud security practices

Table 9-6 Parameter description

Parameter	Description
Scan Time	Time when scans are performed. It can be accurate to the minute.
Random Deviation Time (Seconds)	Random deviation time of the system detection. The value ranges from 0 to 7,200s.
Scan Days	Day in a week when a detection is performed. You can select any days from Monday to Sunday.

Parameter	Description
System Default Baseline Library	The detection baseline has been configured in the system. You only need to select the baseline you want to scan. All parameters are in their default values and cannot be modified.

----End

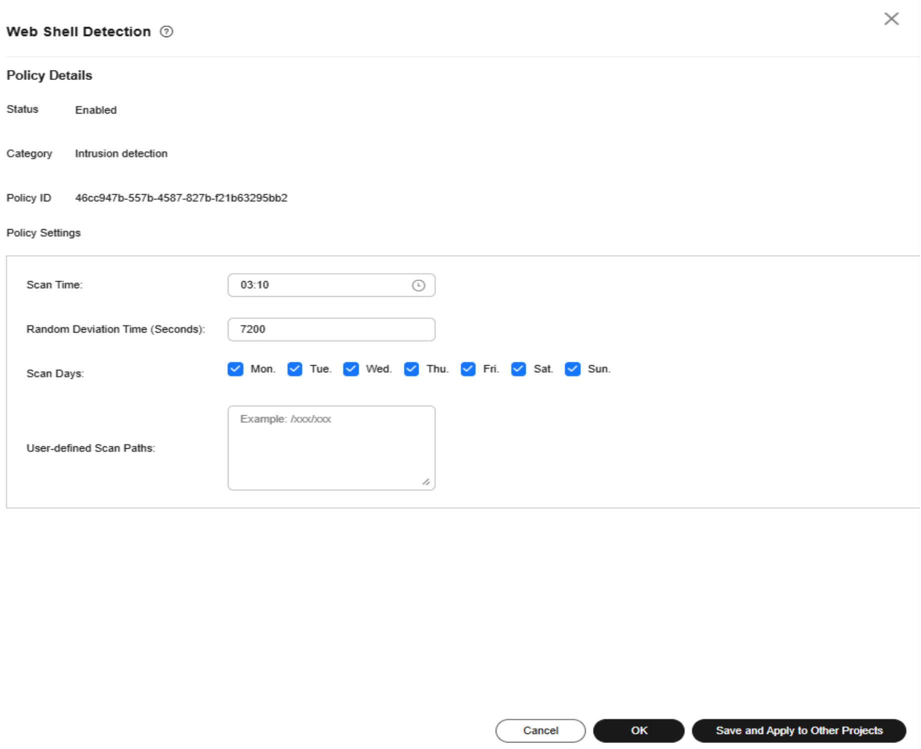
Web Shell Detection

If **User-defined Scan Paths** is not specified, the website paths in your assets are scanned by default. If **User-defined Scan Paths** is specified, website paths and the specified paths are scanned.

Step 1 Click **Web Shell Detection**.

Step 2 On the **Web Shell Detection** page, modify the settings as required. For more information, see **Table 9-7**.

Figure 9-5 Modifying the web shell detection policy



Web Shell Detection

Policy Details

Status Enabled

Category Intrusion detection

Policy ID 46cc947b-557b-4587-827b-f21b63295bb2

Policy Settings

Scan Time: 03:10

Random Deviation Time (Seconds): 7200

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

User-defined Scan Paths: Example: /xxx/xxx

Table 9-7 Parameter description

Parameter	Description
Scan Time	Time point when detections are performed. It can be accurate to the minute.

Parameter	Description
Random Deviation Time (Seconds)	Random deviation time. The value ranges from 0 to 7,200s.
Scan Days	Days in a week when web shells are scanned. You can select one or more days.
User-defined Scan Paths	Web paths to be scanned. A file path must: ● Start with a slash (/) and end with no slashes (/). ● Occupy a separate line and cannot contain spaces. **Do not add network directories as protected directories.** HSS does not scan them even if they are added. The reasons are as follows: 1. A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. 2. The access to network directories may occupy all your bandwidth and affect your services.

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

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

----End

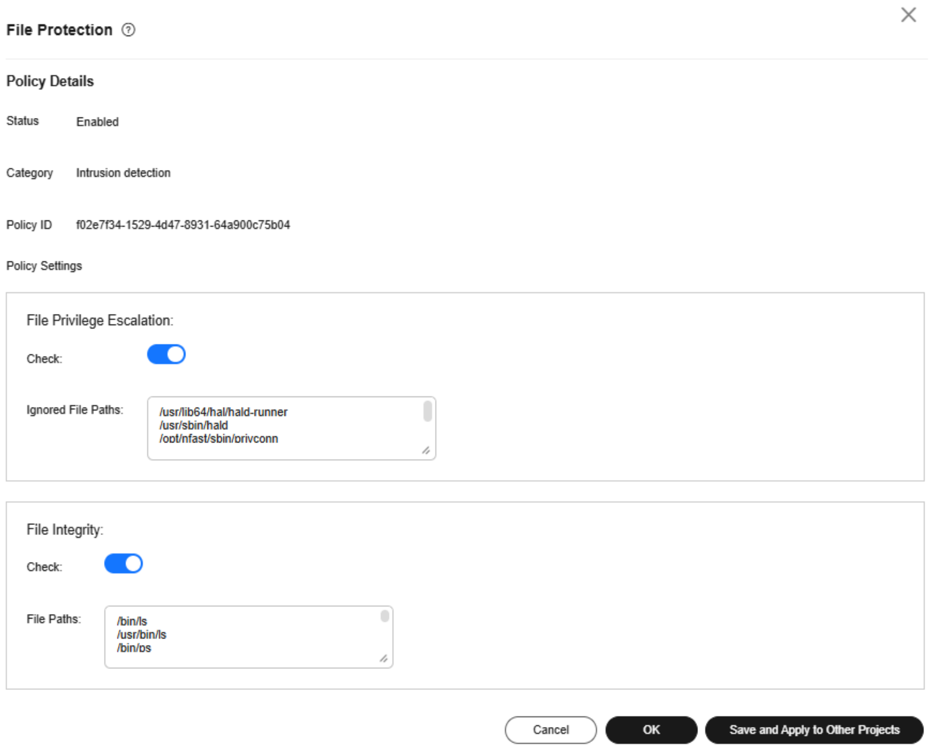
File Protection

Step 1 Click **File Protection**.

Step 2 On the **File Protection** page, modify the policy. For more information, see **Table 9-8**.

The following figure uses the Linux policy as an example.

Figure 9-6 Modifying the file protection policy



File Protection ⓘ

Policy Details

Status Enabled

Category Intrusion detection

Policy ID f02e7f34-1529-4d47-8931-64a900c75b04

Policy Settings

File Privilege Escalation:

Check: ●

Ignored File Paths:

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

File Integrity:

Check: ●

File Paths:

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

Table 9-8 Parameter description

Parameter	Description	Supported OS
File Privilege Escalation	- Detects privilege escalation. This option is enabled by default. – ●: enabled – ○: disabled - **Ignored File Path**: Files to be ignored. Start the path with a slash (/) and do not end it with a slash (/). Each path occupies a line. No spaces are allowed between path names.	Linux
File Integrity	- Checks the integrity of key files. This option is enabled by default. – ●: enabled – ○: disabled - **File Paths**: Configure the file paths.	Linux

Parameter	Description	Supported OS
Important File Directory Change	- Detects the directory change of key files. This option is disabled by default. – ●: enabled – ○: disabled - **Session IP Whitelist**: If the file process belongs to the sessions of the listed IP addresses, no audit applies. - **Unmonitored File Types**: File types that do not need to be monitored. - **Unmonitored File Paths**: File paths that do not need to be monitored. - **Monitoring Login Keys**: monitors login keys. This option is enabled by default. – ●: enabled – ○: disabled	Linux

Parameter	Description	Supported OS
Directory Monitoring Mode for Linux	● Directory monitoring mode. Its value can be **Conservative** or **Sensitive**. The **Conservative** mode has two more attributes (**Monitor Subdirectory** and **Monitor Property Change**) selected by default than the **Sensitive** modes. ● Some file or directory monitoring paths are preset in the system. You can modify the file change type to be detected and add the file or directory paths to be monitored. – **File or Directory Path**: path of the file or directory to be monitored. Up to 50 paths can be added. Ensure the specified paths are valid. **CAUTION** **Do not add network directories as monitored directories.** HSS does not check them even if they are added. The main reasons are as follows: 1. A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. 2. The access to network directories may occupy all your bandwidth and affect your services. – **Alias**: alias of a file or directory path. You can enter a name that is easy to distinguish. – **Monitor Subdirectory**: If this option is selected, all files in the corresponding subdirectories are monitored. If it is not selected, subdirectories are not monitored. – **Monitor Creation**, **Monitor Deletion**, **Monitor Movement**, and **Monitor Modification**: Select them as needed.	Linux

Parameter	Description	Supported OS
Directory Monitoring Mode for Windows	Some file or directory monitoring paths are preset in the system. You can modify the file change type to be detected and add the file or directory paths to be monitored. ● **File or Directory Path**: path of the file or directory to be monitored. Up to 50 paths can be added. Ensure the specified paths are valid. **CAUTION** **Do not add network directories as monitored directories.** HSS does not check them even if they are added. The main reasons are as follows: 1. A network directory usually contains a large number of files and may reach hundreds of terabytes, severely slowing down a scan. 2. The access to network directories may occupy all your bandwidth and affect your services. ● **Alias**: a user-defined name used to distinguish files or directories. Its value has no impact on the monitoring effect. ● **Monitor Subdirectory**: If this option is selected, all files in the subdirectories are monitored. If it is not selected, subdirectories are not monitored. ● **File Name Extension**: type of the file to be monitored. A maximum of 50 extensions can be added. ● **Ignored Path**: Valid if **Monitor Subdirectory** is selected. It specifies the subdirectories that do not need to be monitored. Up to 20 paths can be added. Ensure the specified paths are valid. ● **Monitor Creation**, **Monitor Deletion**, **Monitor Movement**, and **Monitor Modification**: Select them as needed.	Windows

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

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

----End

Graph Engine Detection

Graph engine detection performs comprehensive source tracing analysis based on the threat information provided by multiple modules (including HIPS detection, AI ransomware detection, and antivirus detection). It can associate and comprehensively analyze multiple suspicious process events to identify intrusion behaviors, enhancing defense against vulnerability exploits.

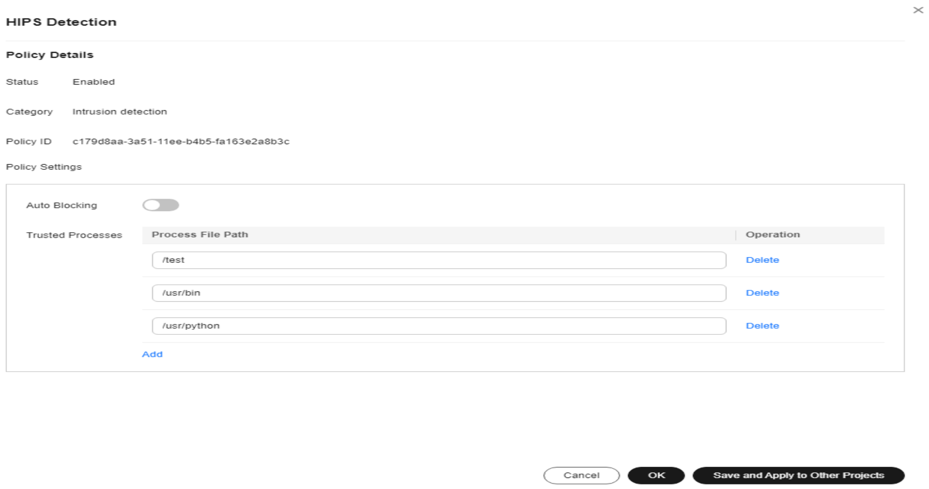
To use the graph engine, you can enable the graph engine detection policy.

HIPS Detection

Step 1 Click **HIPS Detection**.

Step 2 Modify the policy content. For more information, see **Table 9-9**.

Figure 9-7 Modifying the HIPS detection policy



HIPS Detection

Policy Details

Status: Enabled

Category: Intrusion detection

Policy ID: c179d8aa-3a51-11ee-b4b5-fa163e2a8b3c

Policy Settings

Auto Blocking: disabled

Trusted Processes:

Process File Path	Operation
/test	Delete
/usr/bin	Delete
/usr/python	Delete

Table 9-9 Parameter description

Parameter	Description
Auto Blocking	If this function is enabled, abnormal changes on registries, files, and processes will be automatically blocked to prevent reverse shells and high-risk commands. ● ●: enabled ● ○: disabled
Trusted Processes	Paths of trusted processes. You can click **Add** to add a path and click **Delete** to delete it.

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

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

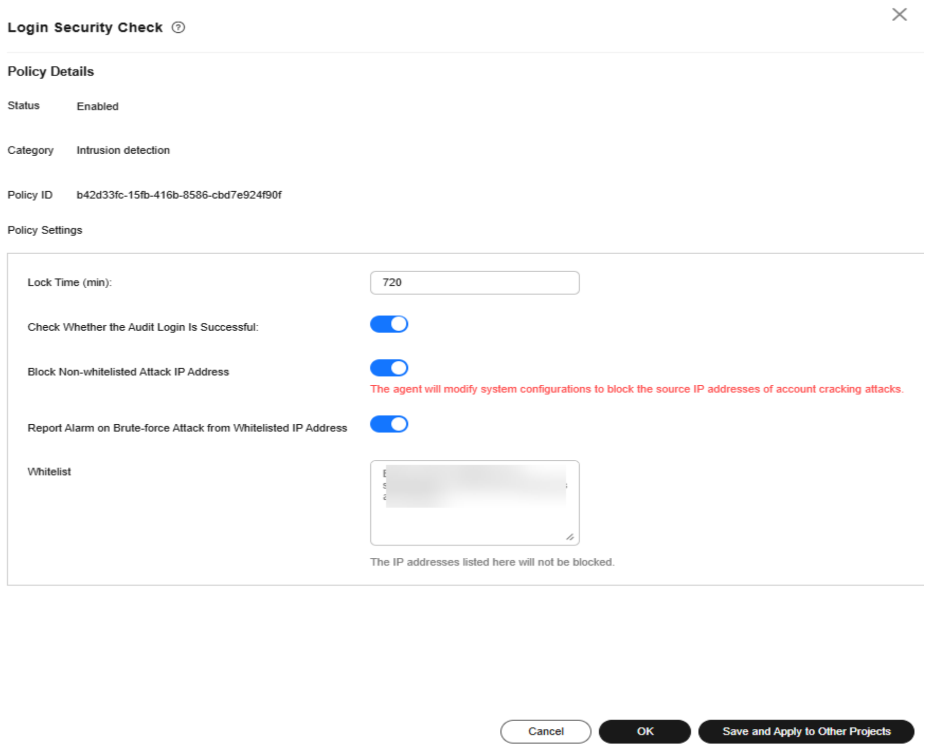
----End

Login Security Check

Step 1 Click **Login Security Check**.

Step 2 On the displayed **Login Security Check** page, modify the policy content. **Table 9-10** describes the parameters.

Figure 9-8 Modifying the security check policy



Login Security Check

Policy Details

Status: Enabled

Category: Intrusion detection

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

Policy Settings

Lock Time (min): 720

Check Whether the Audit Login Is Successful: ⬤

Block Non-whitelisted Attack IP Address: ⬤

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

Report Alarm on Brute-force Attack from Whitelisted IP Address: ⬤

Whitelist: [redacted]

The IP addresses listed here will not be blocked.

Table 9-10 Parameter description

Parameter	Description
Lock Time (min)	This parameter is used to determine how many minutes the IP addresses that send attacks are locked. The value range is 1 to 43200. Login is not allowed in the lockout duration.
Check Whether the Audit Login Is Successful	● After this function is enabled, HSS reports successful logins. – ⬤: enabled – ◯: disabled
Block Non-whitelisted Attack IP Address	After this function is enabled, HSS blocks the login of brute force IP addresses (non-whitelisted IP addresses).
Report Alarm on Brute-force Attack from Whitelisted IP Address	● After this function is enabled, HSS generates alarms for brute force attacks from whitelisted IP addresses. – ⬤: enabled – ◯: disabled

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

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

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

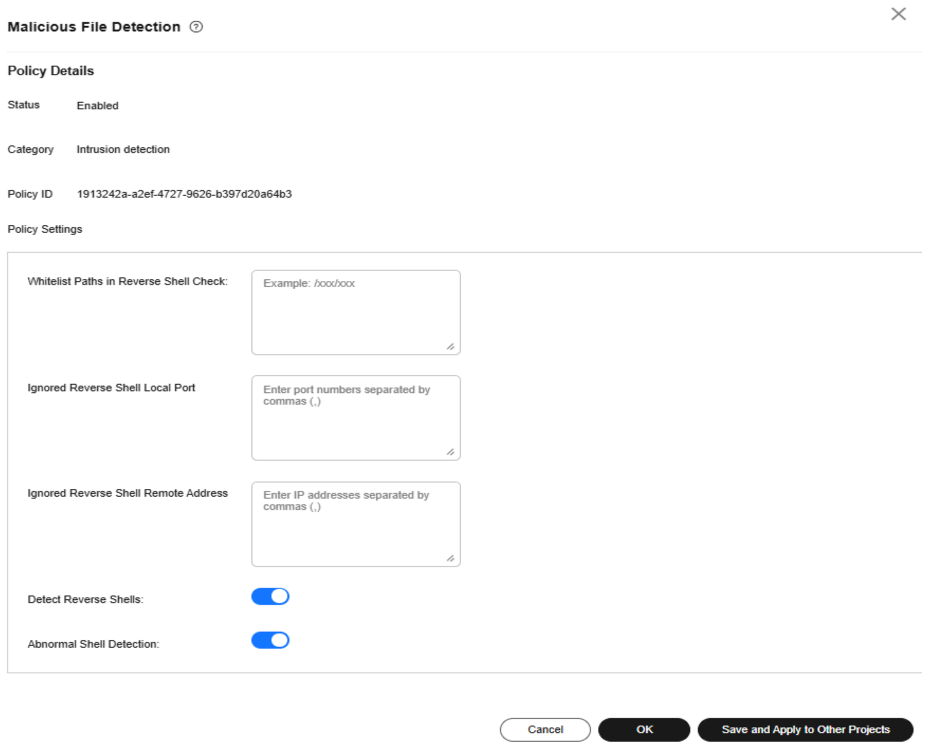
----End

Malicious File Detection

Step 1 Click **Malicious File Detection**.

Step 2 On the displayed page, modify the policy. For more information, see **Table 9-11**.

Figure 9-9 Modifying the malicious file detection policy



Malicious File Detection

Policy Details

Status Enabled

Category Intrusion detection

Policy ID 1913242a-a2ef-4727-9626-b397d20a64b3

Policy Settings

Whitelist Paths in Reverse Shell Check: Example: /xxx/xxx

Ignored Reverse Shell Local Port Enter port numbers separated by commas (,)

Ignored Reverse Shell Remote Address Enter IP addresses separated by commas (,)

Detect Reverse Shells: ●

Abnormal Shell Detection: ●

Table 9-11 Parameter description

Parameter	Description
Whitelist Paths in Reverse Shell Check	Process file path to be ignored in reverse shell detection Start with a slash (/) and end with no slashes (/). Occupy a separate line and cannot contain spaces.
Ignored Reverse Shell Local Port	Local ports that do not need to be scanned for reverse shells.
Ignored Reverse Shell Remote Address	Remote addresses that do not need to be scanned for reverse shells.
Detect Reverse Shells	● Whether to enable reverse shell detection. It monitors the process behavior of users in real time, and can detect and block the reverse shell behaviors from unauthorized shell connections. You are advised to enable this function. – ●: enabled – ○: disabled
Abnormal Shell Detection	● Whether to enable abnormal shell detection. It checks for actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. You are advised to enable this function. – ●: enabled – ○: disabled

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

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

----End

Abnormal Process Behaviors

The abnormal process behavior policy supports two detection modes:

- Sensitive: In-depth full scans are performed on all processes, which may cause false positives. Suitable for network protection drills and key event assurance.
- Balanced: All processes are scanned. The scan result accuracy and the abnormal process detection rate are moderate. Suitable for routine protection.

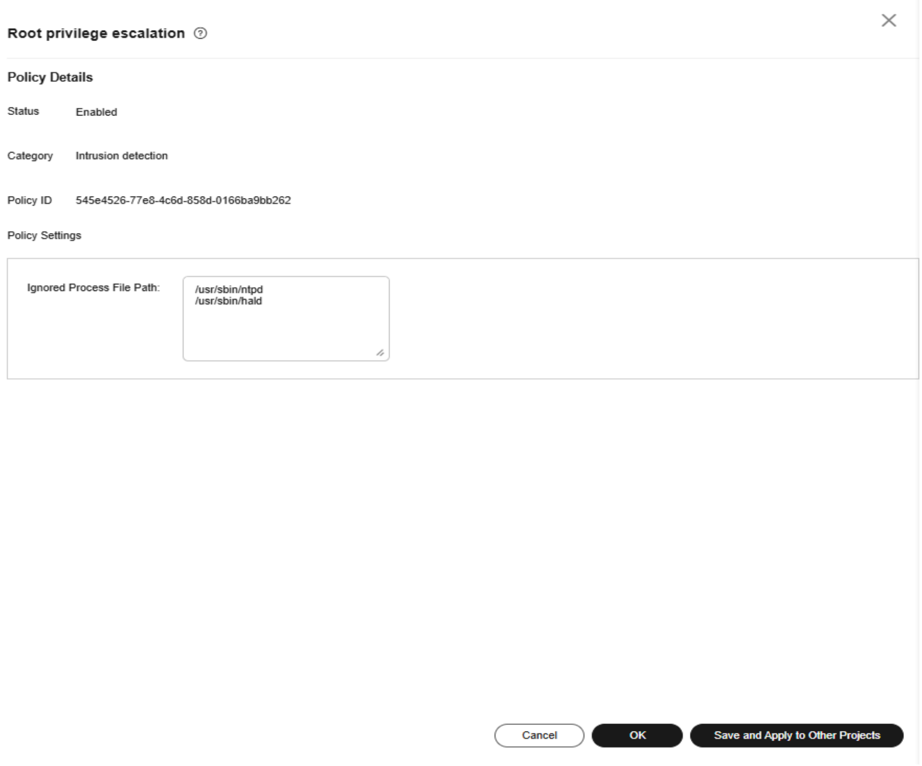
This policy does not need to be configured separately. It changes with the protection mode of the policy group. To enable the sensitive mode, change the protection mode of the policy group to **Sensitive** by referring to **Configuring the Policy Group Protection Mode**.

Root Privilege Escalation Detection

Step 1 Click **Root privilege escalation**.

Step 2 In the displayed area, modify the settings as required. For more information, see **Table 9-12**.

Figure 9-10 Modifying the root privilege escalation policy



Root privilege escalation

Policy Details

Status Enabled

Category Intrusion detection

Policy ID 545e4526-77e8-4c6d-858d-0166ba9bb262

Policy Settings

Ignored Process File Path: /usr/sbin/ntpd
/usr/sbin/hald

Table 9-12 Parameter description

Parameter	Description
Ignored Process File Path	Ignored process file path Start with a slash (/) and end with no slashes (/). Occupy a separate line and cannot contain spaces.

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

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

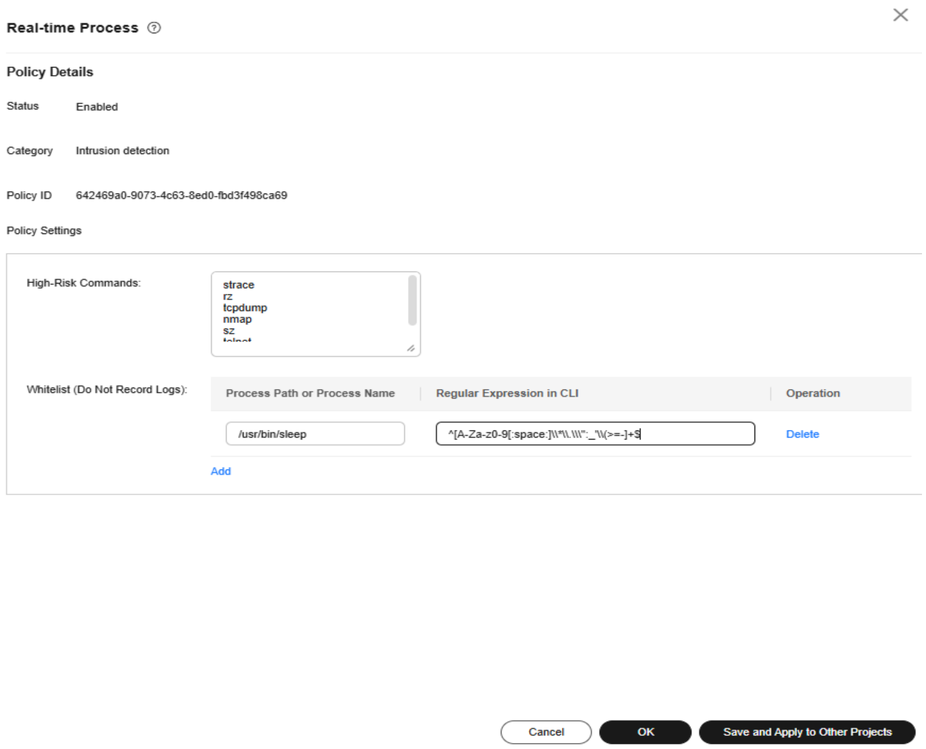
----End

Real-time Process

Step 1 Click **Real-time Process**.

Step 2 On the displayed page, modify the settings as required. For more information, see **Table 9-13**.

Figure 9-11 Modifying the real-time process policy



Real-time Process

Policy Details

Status Enabled

Category Intrusion detection

Policy ID 642469a0-9073-4c63-8ed0-fbd3f498ca69

Policy Settings

High-Risk Commands:

```
strace
rz
tcpdump
nmap
sz
```

Whitelist (Do Not Record Logs):

Process Path or Process Name	Regular Expression in CLI	Operation
/usr/bin/sleep	^[A-Za-z0-9[:space:]\\*\\.\\\":_'\\(>=-]+$	Delete

Table 9-13 Parameters for real-time process policy settings

Parameter	Description
High-Risk Commands	High-risk commands that contain keywords. The command can contain only letters, numbers, hyphens (-), spaces, and the following special characters: /* \=>.:'"+- Currently, built-in shell commands cannot be detected.
Whitelist (Do Not Record Logs)	Paths or programs that are allowed or ignored during detection. You can enter the regular expression of the command to be added to the whitelist. The command regular expression is optional. Example: ● Full path or program name of a process: /usr/bin/sleep ● Command regular expression: ^[A-Za-z0-9[:space:]\\*\\.\\\":_'\\(>=-]+$

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

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

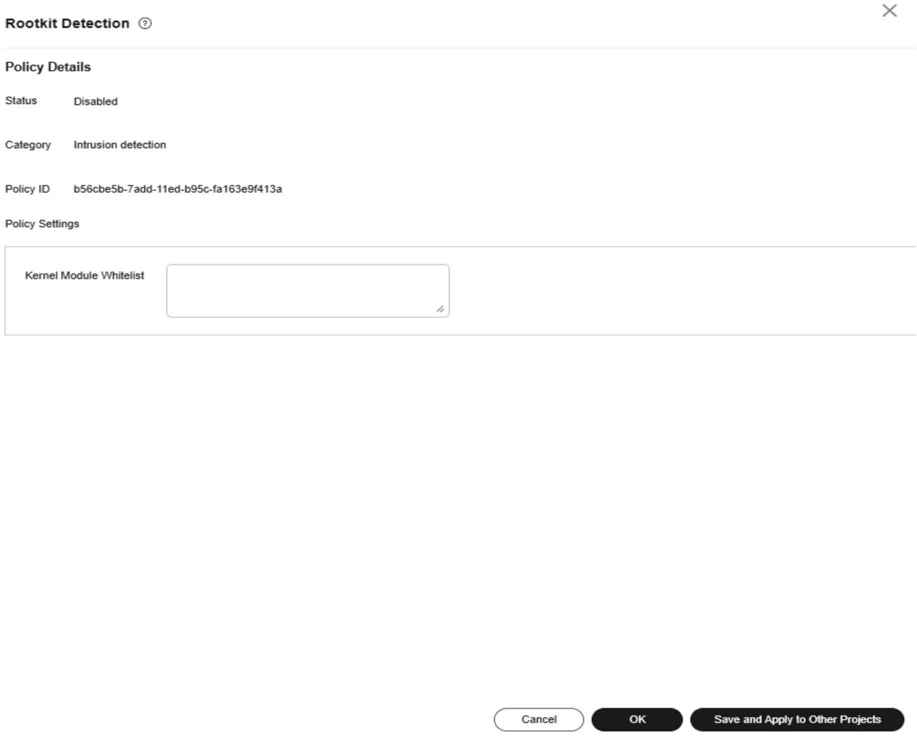
----End

Rootkit Detection

Step 1 Click **Rootkit Detection**.

Step 2 On the rootkit detection page, modify the policy content.

Figure 9-12 Modifying the rootkit detection policy



Rootkit Detection

Policy Details

Status Disabled

Category Intrusion detection

Policy ID b56cbe5b-7add-11ed-b95c-fa163e9f413a

Policy Settings

Kernel Module Whitelist

Table 9-14 Parameter description

Parameter	Description	Example Value
Kernel Module Whitelist	Add the kernel modules that can be ignored during the detection. Up to 10 kernel modules can be added. Each module occupies a line.	xt_conntrack virtio_scsi tun

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

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

----End

AV Detection

Step 1 Click **AV Detection**.

Step 2 On the **AV Detection** slide pane that is displayed, modify the settings as required. For details, see **Table 9-15**.

Table 9-15 Parameter description

Parameter	Description	Example Value
Real-Time Protection	After this function is enabled, AV detection is performed in real time when the current policy is executed. You are advised to enable this function. ● ◉: enabled ● ○: disabled	◉: enabled
Protected File Type	Type of the files to be checked in real time. ● **All**: Select all file types. ● **Executable**: Executable file types such as EXE, DLL, and SYS. ● **Compressed**: Compressed file types such as ZIP, RAR, and JAR. ● **Text**: Text file types such as PHP, JSP, HTML, and Bash. ● **OLE**: Composite file types such as Microsoft Office files (PPT and DOC) and saved email files (MSG). ● **Other**: File types except the preceding types.	All
Action	Handling method for the object detection alarms. ● **Automated handling**:Isolate high-risk virus files bu default. Report other virus files but do not isolate them. ● **Manual handling**: Report all the detected virus files but do not isolate them. You need to handle them manually.	Automatic handling

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

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

----End

Container Information Collection

Step 1 Click **Container Information Collection**.

Step 2 On the **Container Information Collection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 9-16**.

Table 9-16 Container information collection policy parameters

Parameter	Description	Example Value
Mount Path Whitelist	Enter the directory that can be mounted. The whitelist has a higher priority than blacklist. If a directory is specified in both the whitelist and blacklist, it is regarded as a whitelisted item.	/test/docker or /root/* Note: If a directory ends with an asterisk (*), it indicates all the sub-directories under the directory (excluding the main directory). For example, if **/var/test/*** is specified in the whitelist, all sub-directories in **/var/test/** are whitelisted, excluding the **test** directory.
Mount Path Blacklist	Enter the directories that cannot be mounted. For example, **user** and **bin**, the directories of key host information files, are not advised being mounted. Otherwise, important information may be exposed.	

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

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

----End

Cluster Intrusion Detection

Step 1 Click **Cluster Intrusion Detection**.

Step 2 On the **Cluster Intrusion Detection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 9-17**.

Table 9-17 Cluster intrusion detection policy parameters

Parameter	Description	Example Value
Basic Detection Cases	You can select check items as needed. The options are as follows: - **High-privilege RoleBinding**: Check for high-privilege role binding behaviors. **RoleBinding** binds an account to a role. Hackers can bind a common account to a high-privilege role to obtain permissions. - **High-privilege ClusterRoleBinding**: Check for high-privilege cluster role binding behaviors. **ClusterRoleBinding** binds an account to a cluster role. Hackers can bind a common account to a high-privilege role to obtain permissions. - **ServiceAccount creations**: Checks for the creation of service accounts. Service accounts are important Kubernetes credentials. Hackers can create service accounts and bind them to high-privilege roles to control clusters. - **List Secrets operations**: Check for List Secrets operations. Kubernetes Secret is an object that allows users to store and manage sensitive information (such as passwords and connection strings) in a cluster. List Secrets can be referenced in the pod configuration. Attackers who have the permission to retrieve secrets from the API server (for example, by using the service account of the pod) can access sensitive information, which may include the credentials of diverse services. - **DaemonSet creations**: Check for DaemonSet creations. Attacker may attempt to run their code in a cluster by creating a new container. DaemonSet is the best way to control all nodes in Kubernetes. - **Cronjob creation**: Check for Cronjob creations. Kubernetes jobs can be used to run containers that execute	Select all

Parameter	Description	Example Value
	batch processing tasks. These tasks are usually limited. - **Interactive shell used for exec in pods**: Check for the exec using an interactive shell in a pod. Hackers may use interactive shell programs such as bash and sh to perform operations in containers. - **Privileged pod creations**: Check for privileged pod creations. Creating a privileged container and escaping from it is one of the most common escape methods. - **Pods created with sensitive directory**: Check for the creation of pods containing sensitive directories. Hackers may mount sensitive directories, such as **/**, **/root**, and **/etc**, to servers to escalate permissions. - **Pods created with host network namespace**: Check for the creation of pods with a host network namespace. Hackers may create containers that use the host network to escape or listen to traffic. - **Pods created with host PID space**: Check for the creation of pods with a server PID space. Hackers may create containers with a server PID namespace to escape. - **Unauthorized access to API server**: Check for unauthorized access to the API server. Hackers may send API requests to probe the cluster and obtain information about containers, secrets, and other resources in the cluster. These probing behaviors usually trigger alarms for unauthorized access to the API server. - **Access to API Server with curl**: Check for the use of curl to access the API server. Generally, tools like kubectl are unlikely to exist in containers. Using curl to intrude pods and probe API servers is one of the most common attack methods.	

Parameter	Description	Example Value
	- **Exec in system management space** : Check for the **exec** command used for management components such as kube-apiserver. - **Ingress vulnerability**: Check for ingress vulnerabilities. Users who can create or update ingress objects can use custom fragments to obtain all the secrets in the cluster. - **Ingress-alias**: Check for ingress aliases. Users who have the permissions to create or update ingress objects can use the **spec.rules[].http.paths[].path** field in an ingress object (in the **networking.k8s.io** or **extensions** API group) to obtain the credential of the ingress-nginx controller. By default, the credential has access to all confidential information in the cluster. - **SelfSubjectRulesReview**: Check for the behaviors of querying SelfSubjectRulesReview. When a hacker enters a pod, the hacker needs to check the service account (SA) rights of the pod or the token rights stolen through the pod. - **Pods created in management space**: Check for the pod creations in the system management space. Generally, after a Kubernetes cluster becomes stable, the resources in the kube-system namespace will not be created or deleted randomly. Attackers usually forge management components to implement persistence operations. - **Static pod creations**: Check for static pod creations. Hackers may use static pods to achieve a certain purpose, because static pods cannot be deleted through the API server. - **Man-in-the-middle attack**: Check for man-in-the-middle (MITM) attacks and medium-risk vulnerabilities (such as CVE-2020-8554).	

Parameter	Description	Example Value
	● **Worm, mining, or Trojan**: Check for the pods created using the images infected with worms, mining software, or Trojans. ● **K8s event deletion**: Check for Kubernetes event deletions. Kubernetes events help to identify changes that have occurred in a cluster. Attackers may want to delete these events (for example, by using the **kubectl delete events --all** command) so that their activities in the cluster cannot be detected.	
Whitelist	You can customize the types and values that need to be ignored during the detection. You can add and delete types and values as required. The following types are supported: ● IP address filter ● Pod name filter ● Image name filter ● User filter ● Pod tag filter ● Namespace filter	Type: IP address filtering Value: 192.168.x.x

Step 3 Click **OK**.

- If **All projects** are selected for an enterprise project and the policy of the default policy group is modified, you can click **Save and Apply to Other Projects** to apply the modification to other policies of the same edition.
- After this policy is configured, you need to enable log audit and deploy the HSS agent on the management node (node where the APIServer is located) of the cluster to apply the policy.

----End

Container Escape Detection

Step 1 Click **Container Escape**. The container escape policy details page is displayed.

Step 2 On the container escape page that is displayed, edit the policy content. For details about the parameters, see **Table 9-18**.

If no image, process, or POD needs to be added to the whitelist, leave the whitelist blank.

Table 9-18 Container escape detection policy parameters

Parameter	Description
Image Whitelist	Enter the names of the images that do not need to perform container escape behavior detection. An image name can contain only letters, numbers, underscores (_), and hyphens (-), and each name needs to be on a separate line. Up to 100 image names are allowed.
Process Whitelist	Enter the full paths of processes that do not need to perform container escape behavior detection. A process path can contain only letters, numbers, underscores (_), and hyphens (-), and each path needs to be on a separate line. Up to 100 process paths are allowed.
Pod Name Whitelist	Enter the names of pods that do not need to perform container escape behavior detection. A pod name can contain only letters, numbers, underscores (_), and hyphens (-), and each name needs to be on a separate line. Up to 100 pod names are allowed.

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

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

----End

Container Escape Prevention

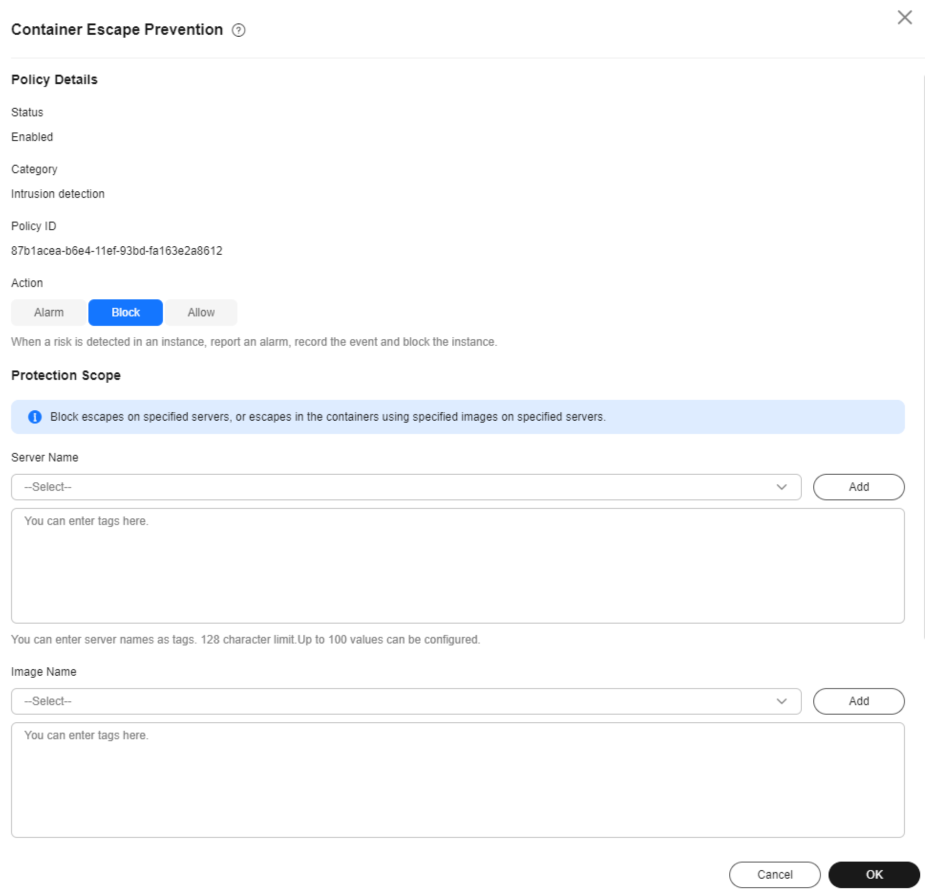
NOTE

This function is in the OBT phase. To use it, **submit a service ticket**.

Step 1 Click **Container Escape Prevention**. The policy details page is displayed.

Step 2 Edit the policy. For details about the parameters, see **Table 9-19**.

Figure 9-13 Container escape prevention policy



Container Escape Prevention

Policy Details

Status

Enabled

Category

Intrusion detection

Policy ID

87b1acea-b6e4-11ef-93bd-fa163e2a8612

Action

Alarm [✓ Block] Allow

When a risk is detected in an instance, report an alarm, record the event and block the instance.

Protection Scope

Block escapes on specified servers, or escapes in the containers using specified images on specified servers.

Server Name

--Select-- Add

You can enter tags here.

You can enter server names as tags. 128 character limit.Up to 100 values can be configured.

Image Name

--Select-- Add

You can enter tags here.

Cancel OK

Table 9-19 Container escape prevention policy parameters

Parameter	Description	Example Value
Action	- **Alarm**: If an abnormal runtime behavior is detected, only an alarm is reported. - **Block**: If an abnormal runtime behavior is detected, an alarm is reported and the container instance is blocked. - **Allow**: If an abnormal runtime behavior is detected, the container instance is still allowed to run.	Block

Parameter	Description	Example Value
Protection Scope	Select the protection scope of abnormal runtime behavior detection. Specify server and image names to detect abnormal behaviors of the containers that use the specified images on specified servers. The configuration methods are as follows: ● **Server Name**: Select a server from the drop-down list and click **Add**. Alternatively, enter a server name in the text box and press **Enter**. Each name can contain up to 128 characters. Up to 100 server names can be configured. ● **Image Name**: Select an image name from the drop-down list and click **Add**. Alternatively, enter an image name in the text box and press **Enter**. Each name can contain up to 128 characters. Up to 100 image names can be configured.	● Server name: **test01** ● Image name: **moby/buildkit buildx-stable-1**

Parameter	Description	Example Value
Policy Settings	The container anti-escape policy contains preset rules detecting abnormal behaviors in processes, files, and system calls. A detection rule specifically a scenario where abnormal behaviors are checked for. It does not define runtime abnormal behaviors. You can enable or disable the detection rule as required. (The rules are disabled by default.) The rule names and IDs are as follows: ● **Escape by Writing in High-risk Directory on Host** (ae246a6fb5290701): Check whether a sensitive host directory is mounted to a container, and a process in the container is used to write data to the directory. ● **Container Escape Tool Execution** (ce246a6fb5290702): Check for the execution of container escape tools such as CDK. ● **User Configuration File Change on Host** (de246a6fb5290703): Check for modifications on the system and application configuration files on a host. ● **High-risk System Call** (ee246a6fb5290704): Check for high-risk system calls, such as **chown**, used by processes. In addition to the preceding detection rules, the HSS can detect abnormal network activities and process capabilities. If an abnormal behavior event triggers a detection rule whose **Action** is **Alarm** or **Block**, the ID of the triggered rule is displayed in the alarm summary reported by HSS. The **Action** of a detection rule is **Alarm** by default, but this setting has a lower priority than the **Action** of the policy. If the policy action is **Block**, the actual rule action will also be **Block**.	Enable all (●)

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

----End

Container Information Module

Step 1 Click **Container Information Collection**.

Step 2 Modify the policy content as prompted. For details about the parameters related to the policy, see **Table 9-20**.

Table 9-20 Container information module policy parameters

Parameter	Description
Custom Container Whitelist	Enter the container name that can be ignored during the detection. ● Simple names of containers can be configured based on Docker. HSS automatically performs fuzzy match. Other containers perform exact match based on their names. ● Each container name needs to be on a separate line. Up to 100 whitelist items are allowed.
Custom Image Organization Whitelist	Enter the organization name that can be ignored during the detection. Each organization name needs to be on a separate line. Up to 100 whitelist items are allowed.

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

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

----End

Container File Monitoring

If a monitored file path is under the mount path rather than the writable layer of the container on the server, changes on the file cannot trigger container file modification alarms. To protect such files, configure a **file protection policy**.

Step 1 Click **Container File Monitoring**.

Step 2 On the **Container File Monitoring** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 9-21**.

Table 9-21 Container file monitoring policy parameters

Parameter	Description	Example Value
Fuzzy Match	Indicates whether to enable fuzzy match for the target file. You are advised to select this option.	Selected
Image Name	Name of the target image to be checked	test_bj4
Image ID	ID of the target image to be checked	-
File	Name of the file in the target image to be checked	/tmp/testw.txt

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

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

----End

Container Process Whitelist

Step 1 Click **Container Process Whitelist**.

Step 2 On the **Container Process Whitelist** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 9-22**.

Table 9-22 Container process whitelist policy parameters

Parameter	Description	Example Value
Dynamic Whitelist	If it is enabled, HSS assumes that a container only runs the process commands configured in its startup parameters. When a container is started, HSS identifies its entrypoint configuration to determine its main process. If other processes are detected running in the container, an alarm will be triggered.	●
Fuzzy Match	Indicates whether to enable fuzzy match for the target file. You are advised to select this option.	Selected
Image Name	Name of the target image to be checked	test_bj4
Image ID	ID of the target image to be checked	sha256:732aab547cfe56841c02fb83921db4b91f04a1e636cc2cad76e224897056f140
Process	Full path of the file in the target image to be checked	/tmp/testw

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

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

----End

Suspicious Image Behaviors

Step 1 Click **Suspicious Image Behaviors**.

Step 2 On the **Suspicious Image Behaviors** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 9-23**.

Table 9-23 Suspicious image behaviors policy parameters

Parameter	Description	Example Value
Rule Name	Name of a rule	-
Description	Brief description of a rule	-
Template	● Configure templates based on different rules. The supported rules are as follows: – Image whitelist – Image blacklist – Image tag whitelist – Image tag blacklist – Create container whitelist – Create container blacklist – Container mount proc whitelist – Container seccomp unconfined – Container privilege whitelist – Container capability whitelist ● The parameters are described as follows: – **Exact match**: Enter the names of the images you want to check. Use semicolons (;) to separate multiple names. A maximum of 20 names can be entered. – **RegEx match**: Use regular expressions to match images. Use semicolons (;) to separate multiple expressions. A maximum of 20 expressions can be entered. – **Prefix match**: Enter the prefixes of the images you want to check. Multiple prefixes are separated by semicolons (;). A maximum of 20 prefixes can be entered. – **Tag Name**: Enter the tag and value of the images you want to check. A maximum of 20 tags can be added. – **Permission Type**: Specify permissions to be checked or ignored. For details about permissions, see **Table 9-24**.	-

Table 9-24 Abnormal image permissions

Permissions Name	Description
AUDIT_WRITE	Write records to kernel auditing log.
CHOWN	Make arbitrary changes to file UIDs and GIDs.
DAC_OVERRIDE	Bypass file read, write, and execute permission checks.
FOWNER	Bypass permission checks on operations that normally require the file system UID of the process to match the UID of the file.
FSETID	Do not clear set-user-ID and set-group-ID permission bits when a file is modified.
KILL	Bypass permission checks for sending signals
MKNOD	Create special files using mknod.
NET_BIND_SERVICE	Bind a socket to internet domain privileged ports (port numbers less than 1024).
NET_RAW	Use RAW and PACKET sockets.
SETFCAP	Set file capabilities.
SETGID	Make arbitrary manipulations of process GIDs and supplementary GID list.
SETPCAP	Modify process capabilities.
SETUID	Make arbitrary manipulations of process UIDs.
SYS_CHROOT	Use chroot to change the root directory.
AUDIT_CONTROL	Enable and disable kernel auditing; change auditing filter rules; retrieve auditing status and filtering rules.
AUDIT_READ	Allow reading audit logs via multicast netlink socket.
BLOCK_SUSPEND	Allow suspension prevention.
BPF	Allow creating BPF maps, loading BPF Type Format (BTF) data, retrieve JITED code of BPF programs, and more.
CHECKPOINT_RESTORE	Allow operations related to checkpoints and restoration.
DAC_READ_SEARCH	Bypass file read permission checks and directory read and execute permission checks.
IPC_LOCK	Lock memory (such as mlock, mlockall, mmap, and shmctl).

Permissions Name	Description
IPC_OWNER	Bypass permission checks for operations on System V IPC objects.
LEASE	Establish leases on arbitrary files
LINUX_IMMUTABLE	Set the FS_APPEND_FL and FS_IMMUTABLE_FL i-node flags.
MAC_ADMIN	Allow MAC configuration or state changes.
MAC_OVERRIDE	Override Mandatory Access Control (MAC).
NET_ADMIN	Perform various network-related operations.
NET_BROADCAST	Make socket broadcasts, and listen to multicasts.
PERFMON	Allow privileged system performance and observability operations using perf_events, i915_perf and other kernel subsystems.
SYS_ADMIN	Perform a range of system administration operations.
SYS_BOOT	Use reboot and kexec_load. Reboot and load a new kernel for later execution.
SYS_MODULE	Load and unload kernel modules.
SYS_NICE	Raise process nice value (nice, set priority) and change the nice value for arbitrary processes.
SYS_PACCT	Enable or disable process accounting.
SYS_PTRACE	Trace arbitrary processes using ptrace.
SYS_RAWIO	Perform I/O port operations (ipl and ioperm).
SYS_RESOURCE	Override resource limits.
SYS_TIME	Set the system clock (settimeofday, stime, and adjtimex) and real-time (hardware) clock.
SYS_TTY_CONFIG	Use vhangup. Employ various privileged ioctl operations on virtual terminals.
SYSLOG	Perform privileged syslog operations.
WAKE_ALARM	Trigger something that will wake up the system.

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

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

----End

Port Scan Detection

Step 1 Click **Port Scan Detection**.

Step 2 On the **Port Scan Detection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see **Table 9-25**.

Table 9-25 Port scan detection policy parameters

Parameter	Description	Example Value
Source IP Address Whitelist	Enter one or multiple IP addresses or IP address ranges. Use commas (,) to separate multiple values. Example: **192.168.0.1,192.168.0.2,192.168.10-192.168.100**	192.168.0.1
Ports to Scan	Details about the port number and protocol type to be detected	-

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

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

----End

External Connection Detection

Step 1 Click **External Connection Detection**. The details page is displayed.

Step 2 On the page that is displayed, modify the policy details. **Table 9-26** describes the parameters.

Table 9-26 Parameters of an external connection detection policy

Parameter	Description	Example Value
Process Whitelist	Traffic is filtered based on process names or process file paths, and the traffic directions in the whitelist.	● Process name or file path: **/usr/local/test** ● Traffic direction: bidirectional
Traffic Whitelist	Traffic is filtered based on source or destination IP addresses, ports, or a combination of them.	-
Collection Protocol	The protocol to be detected. The value can be TCP or UDP.	Select all

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

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

----End

Fileless Attack Detection

Step 1 Click **Fileless attack detection**.

Step 2 On the policy details page, view or modify the policy. The following table describes the parameters.

Table 9-27 Parameters of a fileless attack detection policy

Parameter	Description	Example Value
Process injection	- **Process Injection**: Enable or disable process injection detection. – : enabled – : disabled - **Trustlist Matching Specifications**: Configure how to match the user-defined path trustlist. Click ⌄ to select a match mode. The options are as follows: – Full match, case sensitive – Full match, case-insensitive – Fuzzy matching - **Path trustlist**: Enter the paths that do not need to be checked for process injection. Enter one path on each line.	- - Fuzzy matching - /usr/sbin/hald

Parameter	Description	Example Value
LD hijacking	- **LD hijacking**: Enable or disable LD hijacking detection. – ●: enabled – ○: disabled - **Full process detection**: Enable or disable LD hijacking threat detection for all processes. – ●: enabled – ○: disabled - **Trustlist Matching Specifications**: Configure how to match the user-defined path trustlist. Click ⌄ to select a match mode. The options are as follows: – Full match, case sensitive – Full match, case-insensitive – Fuzzy matching - **Path trustlist**: Enter the paths that do not need to be checked for LD highjacking. Enter one path on each line.	- ● - ● - Fuzzy matching - /usr/sbin/hald
Memory-based process	- **Memory-based process**: Enable or disable memory process detection. – ●: enabled – ○: disabled - **Full process detection**: Enable or disable memory-based process threat detection for all processes. – ●: enabled – ○: disabled - **Trustlist Matching Specifications**: Configure how to match the user-defined path trustlist. Click ⌄ to select a match mode. The options are as follows: – Full match, case sensitive – Full match, case-insensitive – Fuzzy matching - **Path trustlist**: Enter the paths that do not need to be checked for memory-based processes. Enter one path on each line.	- ● - ● - Fuzzy matching - /usr/sbin/hald

Parameter	Description	Example Value
VDSO Hijacking	**VDSO Hijacking**: Enable or disable VDSO hijacking detection. - ●: enabled - ○: disabled	●

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

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

----End

Self-protection

The self-protection policy protects HSS software, processes, and files from being damaged by malicious programs. You cannot customize the policy content.

9.1.3 Configuring the Policy Group Protection Mode

Scenario

There are two policy group protection modes. You can choose from them as needed.

- Sensitive mode: applicable to high security scenarios, such as network protection drills and key event security assurance. It achieves a high threat detection rate.
- Balanced mode: applicable to routine protection scenarios. The threat detection rate and accuracy are relatively balanced.

For details about the differences between the two modes, see **Policy Group Protection Modes**.

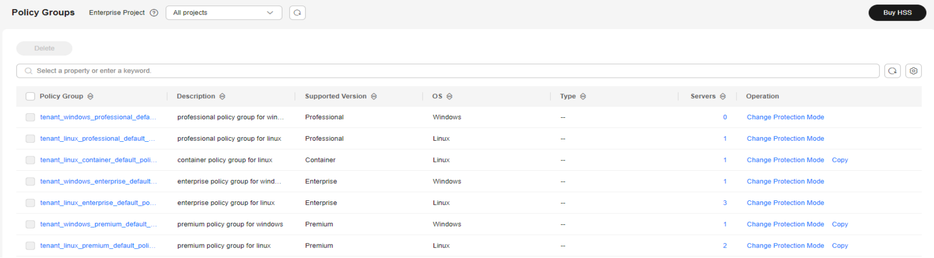
Configuring the Policy Group Protection Mode

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

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

Step 3 In the navigation tree on the left, choose **Security Operations** > **Policies**

Figure 9-14 Policy management



Policy Group	Description	Supported Version	OS	Type	Servers	Operation
tenant_windows_professional_defa...	professional policy group for win...	Professional	Windows	--	0	Change Protection Mode
tenant_linux_professional_default_...	professional policy group for linux	Professional	Linux	--	1	Change Protection Mode
tenant_linux_container_default_poli...	container policy group for linux	Container	Linux	--	1	Change Protection Mode Copy
tenant_windows_enterprise_default...	enterprise policy group for wind...	Enterprise	Windows	--	1	Change Protection Mode
tenant_linux_enterprise_default_po...	enterprise policy group for linux	Enterprise	Linux	--	3	Change Protection Mode
tenant_windows_premium_default_...	premium policy group for windows	Premium	Windows	--	1	Change Protection Mode Copy
tenant_linux_premium_default_poli...	premium policy group for linux	Premium	Linux	--	2	Change Protection Mode Copy

Step 4 In the **Operation** column of the target policy group, click **Change Protection Mode**.

Step 5 In the dialog box that is displayed, select a protection mode and click **OK**.

----End

9.1.4 Creating a Custom Policy Group

Scenario

For premium and container editions, you can copy a policy group and customize it as required to meet server security requirements in different application scenarios.

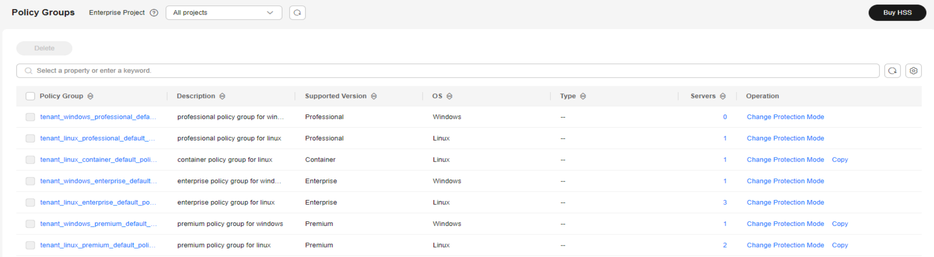
Creating a Custom Policy Group

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Security Operation** > **Policies**. On the displayed page, Policy group parameters describes the fields.

Figure 9-15 Policy management



Policy Group	Description	Supported Version	OS	Type	Servers	Operation
tenant_windows_professional_defa...	professional policy group for win...	Professional	Windows	--	0	Change Protection Mode
tenant_linux_professional_default_...	professional policy group for linux	Professional	Linux	--	1	Change Protection Mode
tenant_linux_container_default_poli...	container policy group for linux	Container	Linux	--	1	Change Protection Mode Copy
tenant_windows_enterprise_default...	enterprise policy group for wind...	Enterprise	Windows	--	1	Change Protection Mode
tenant_linux_enterprise_default_po...	enterprise policy group for linux	Enterprise	Linux	--	3	Change Protection Mode
tenant_windows_premium_default_...	premium policy group for windows	Premium	Windows	--	1	Change Protection Mode Copy
tenant_linux_premium_default_poli...	premium policy group for linux	Premium	Linux	--	2	Change Protection Mode Copy

Table 9-28 Policy group parameters

Parameter	Description
Policy Group	Name of a policy group The preset policy group names are as follows: ● **tenant_linux_advanced_default_policy_group**: preset policy of the Linux professional edition, which can only be viewed but cannot be copied or deleted. ● **tenant_windows_advanced_default_policy_group**: preset policy of the Windows professional edition, which can only be viewed but cannot be copied or deleted. ● **tenant_linux_container_default_policy_group**: preset Linux policy of the container edition. You can copy this policy group and create a new one based on it. ● **tenant_linux_enterprise_default_policy_group** is the default Linux policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. ● **tenant_windows_enterprise_default_policy_group**: preset Windows policy of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted. ● **tenant_linux_premium_default_policy_group**: preset Linux policy of the premium edition. You can create a policy group by copying this default group and modify the copy. ● **tenant_windows_premium_default_policy_group**: preset Windows policy of the premium edition. You can create a policy group by copying this default group and modify the copy. ● **wtp_***ServerName* is a WTP edition policy group. It is generated by default when WTP is enabled for a server.
Description	Detailed description of a policy group.
Supported Version	HSS edition supported by a policy group.
Supported OS	OS supported by a policy group.
Associated Servers	To view details about the servers associated with a policy group, click the number in the **Servers** column of the group.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Select a premium or container edition policy group and click **Copy** in the **Operation** column of the policy group.

Step 6 In the dialog box displayed, enter a policy group name and description, and click **OK**.

- The name of a policy group must be unique, or the group will fail to be created.
- The policy group name and its description can contain only letters, numbers, underscores (_), hyphens (-), and spaces, and cannot start or end with a space.

Step 7 Click **OK**.

After a policy group is created, you can configure rules for each policy in the policy group. For details, see **Configuring Policies**.

----End

Follow-up Procedure

After creating a policy group and configuring policies, you can apply the new policy group to servers. For details, see **Deploying a Protection Policy**.

9.1.5 Deleting a Custom Policy Group

Scenario

Preset policy groups cannot be deleted. You can delete custom policy groups of premium and container editions.

Precautions

After a policy group is deleted, the **Policy Group** column of the servers that were associated with the group will be blank. You need to deploy a policy group for a server again by referring to **Deploying a Protection Policy**.

Deleting a Policy Group

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

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

Step 3 In the navigation tree on the left, choose **Security Operations** > **Policies**

Step 4 Click **Delete** in the **Operation** column of the target policy.

You can also select multiple policies and click **Delete** in the upper left corner of the policy list to delete multiple policy groups in batches.

Step 5 Click **OK**.

----End

9.2 Handling History

You can check the handling history of vulnerabilities, alarms, container events, and virus-infected files, including their handlers and handling time.

Constraints

- The basic edition does not support this function. For details about how to buy and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.
- Handling history can be retained for a maximum of 180 days.

Viewing the Handling History

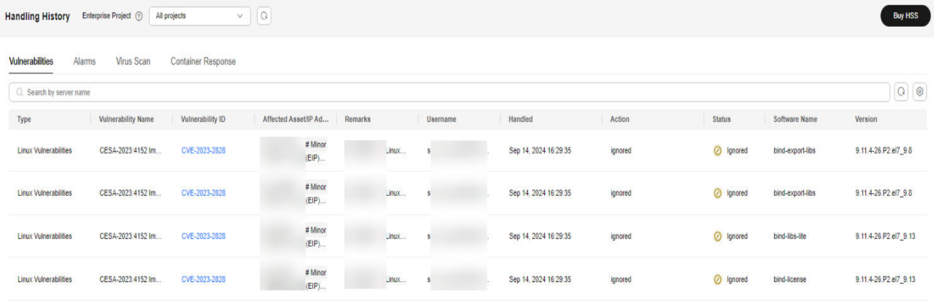
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane on the left, choose **Security Operations** > **Handling History**.

Step 4 Click a tab and view the corresponding historical handling records.

Figure 9-16 Viewing the handling history



Handling History Enterprise Project All projects

Buy HSS

Vulnerabilities Alarms Virus Scan Container Response

Search by server name

Type	Vulnerability Name	Vulnerability ID	Affected Asset/IP Ad...	Remarks	Username	Handled	Action	Status	Software Name	Version
Linux Vulnerabilities	CESA-2023:4152 Im...	CVE-2023-2828	[redacted] # Minor (EIP)...	[redacted] Linux...	s [redacted]	Sep 14, 2024 16:29:35	ignored	Ignored	bind-export-libs	9.11.4-26.P2.el7_9.8
Linux Vulnerabilities	CESA-2023:4152 Im...	CVE-2023-2828	[redacted] # Minor (EIP)...	[redacted] Linux...	s [redacted]	Sep 14, 2024 16:29:35	ignored	Ignored	bind-export-libs	9.11.4-26.P2.el7_9.8
Linux Vulnerabilities	CESA-2023:4152 Im...	CVE-2023-2828	[redacted] # Minor (EIP)...	[redacted] Linux...	s [redacted]	Sep 14, 2024 16:29:35	ignored	Ignored	bind-libs-lite	9.11.4-26.P2.el7_9.13
Linux Vulnerabilities	CESA-2023:4152 Im...	CVE-2023-2828	[redacted] # Minor (EIP)...	[redacted] Linux...	s [redacted]	Sep 14, 2024 16:29:35	ignored	Ignored	bind-license	9.11.4-26.P2.el7_9.13

- Viewing the handling history of a specified enterprise project

  In the upper left corner of the **Handling History** page, select an enterprise project for **Enterprise Project** to view the handling history under the enterprise project.

- Viewing the handling history of a specified attribute

  In the search box above the list, select an attribute or enter a keyword to search for the handling records of a specified attribute.

- Export the handling history to the local PC

  In the upper left corner of the tab page, click **Export**.

  Up to 200,000 historical records can be exported at a time. Exporting more than 5,000 records may take a long time.

----End

9.3 Container Audit

9.3.1 Container Audit Overview

What Is Container Audit?

Keep track of the operations and activities in your container clusters, gaining insight into every phase of the container lifecycle, including creating, starting, stopping, and destroying containers; as well as the communication and transmission between containers. Find and handle security problems through audit and analysis in a timely manner, ensuring the security and stability of container clusters.

Audit Objects

- Cluster container: Kubernetes audit logs, Kubernetes events, container logs, and container commands
- Independent container: container logs and container commands
- SWR image repository: image repository logs

Scenario

If an abnormal operation or activity occurs in the container environment, you can analyze container audit logs to locate the occurrence time, track the event, and work out a solution.

Description

To enable container audit, the following conditions must be met:

1. The cluster container or independent container has been connected to HSS, and is protected by the container edition.

   For more information, see **Installing an Agent in a Cluster** and **Enabling Container Protection**.

2. Meet the prerequisites for certain audit objects, as shown in **Table 9-29**.

Table 9-29 Audit prerequisites

Object	Audit Object	Audit Prerequisite
User-built or third-party cloud cluster	Kubernetes audit logs	1. Enable the cluster intrusion detection policy. For details, see **Configuring Policies**. 2. Enable API server audit. For details, see **Enabling the API Server Audit Function.**

Object	Audit Object	Audit Prerequisite
Huawei Cloud CCE clusters	Kubernetes audit logs	On the CCE console, enable the collection of Kubernetes events, Kubernetes audit logs, and container logs. For details, see **Configuring CCE Logs**.
	Kubernetes audit events	
	Container logs	
SWR private image repository	Image repository logs	You have used SWR and granted the operation permission (**CTSOperatePolicy**) for HSS. For details, see **Authorization**.

After container audit is enabled, operation and activity logs in the cluster are recorded on the HSS console. For details about how to view audit logs, see **Viewing Container Audit Logs**.

9.3.2 Viewing Container Audit Logs

Scenario

This section describes how to view container audit logs.

Viewing Container Audit Logs

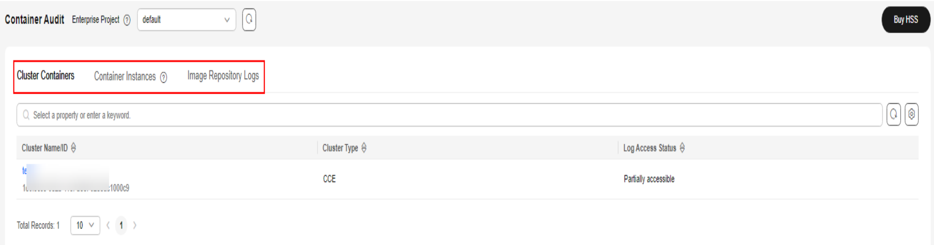
Step 1 **Log in to the management console**.

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

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

Step 4 Perform the following operations to view different types of audit logs:

Figure 9-17 Viewing container audit logs



Container Audit Enterprise Project ⓘ default

Cluster Name/ID	Cluster Type	Log Access Status
[redacted]1000c9	CCE	Partially accessible

Total Records: 1 10 < 1 >

- Viewing cluster container audit logs
  a. Click the **Cluster Containers** tab.
  b. Click the name of a cluster. On the audit details page, view Kubernetes audit logs, Kubernetes events, container logs, and container command records.
- Viewing container instances

a. Click the **Container Instances** tab.

b. Click the name of a container instance. On the audit details page, view container logs and container command records.

- Viewing image repository logs

  Click the **Image Repository Logs** tab to view the audit logs of image repositories.

----End

9.4 Security Report

9.4.1 Security Report Overview

HSS provides daily, weekly, and monthly security reports, and allows you to customize the report period. The reports show the statistics on the security trend, key events, and risks of protected servers.

Constraints

- Security reports are available in HSS professional, enterprise, premium, WTP, and container editions. For details about how to purchase and upgrade HSS, see **Purchasing an HSS Quota** and **Upgrading a Protection Quota**.
- A report will be retained for six months after generation to meet DJCP MLPS and audit requirements.

Security Report Description

By default, weekly and monthly reports are preconfigured in HSS. After protection is enabled for your assets, reports are automatically generated by default. The report content and generation time are as follows:

- Report content:
  - Security overview: risk trend, risk distribution, top 5 unsafe servers, and top 5 brute-force attack sources
  - Risk management: vulnerability statistics, asset account change records, dangerous open ports, and weak passwords
  - Intrusion detection: unsafe accounts, remote login, malicious programs, web shells, account cracking, and key file changes
- Report generation time:
  - A default weekly security report is generated between 06:00 and 12:00 every Monday. It contains the statistics of a week, from 00:00 on Monday to 24:00 on Sunday.
  - A default monthly security report is generated between 06:00 and 12:00 every Monday. It contains the statistics generated from 00:00 on the first day to 24:00 on the last day of a month.

You can view security reports. For details, see **Checking a Security Report**.

If the default report does not meet your requirements, you can create a custom report or edit the default report. For details, see **Creating a Security Report** and **Editing a Report**.

9.4.2 Creating a Security Report

If the type and content of the existing report template cannot meet your requirements, you can customize a report.

Creating a Security Report

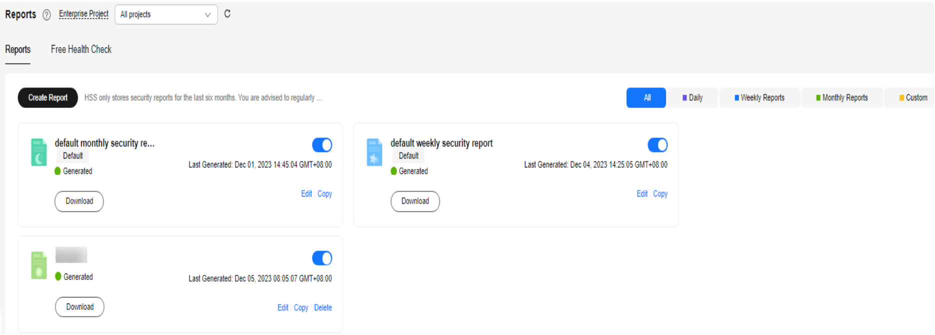
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Figure 9-18 Checking a security report



HSS only stores security reports for the last six months. You are advised to regularly ...

Last Generated: Dec 01, 2023 14:45:04 GMT+08:00

Last Generated: Dec 04, 2023 14:25:05 GMT+08:00

[redacted]

Last Generated: Dec 05, 2023 08:05:07 GMT+08:00

Step 4 Create a report.

- Create a monthly or weekly security report based on templates.
  - Click **Copy** in the weekly or monthly report card to access the basic information configuration page.
- You can also customize the report period.
  - Click **Create Report** to access the basic information configuration page.

Step 5 Edit basic information of a report. For more information, see **Table 9-30**.

Table 9-30 Parameter description

Parameter	Description	Example Value
Report Name	Default report name	ecs security report

Parameter	Description	Example Value
Report Type	Statistical period type of a report: ● **Daily**: 00:00 to 24:00 every day ● **Weekly Reports**: 00:00 on Monday to 24:00 on Sunday ● **Monthly Reports**: 00:00 on the first day to 24:00 on the last day of each month ● **Custom**: custom statistical period, which ranges from one day to three months ● All types of reports will be sent to the recipients the day after it is generated.	Monthly Reports
Schedule Delivery	Time when a report is automatically sent	-
Send Report To	Security report recipients. ● **Recipients specified in Message Center**: If you use Message Center settings, alarm notifications will be sent to the recipients specified in the **Security events** message type. You need to log in to the console and check the mailbox in the upper right corner. ● **Recipients specified in SMN topic**: If you use SMN topic settings, you can create a topic and specify recipients for HSS. ● **No need to send to email**: The report is not sent to the specified email address.	Recipients specified in SMN topic
Report Logo	Logo used in the report. ● **None**: The report does not use any logo. ● **Default** logo: Huawei Cloud logo is used by default. ● **Custom**: Upload a custom logo image. The image cannot exceed 20 KB. Only JPG, PNG, JPEG, and BMP are supported.	None

Step 6 After confirming that the information is correct, click **Next** in the lower right corner of the page to configure the report.

Step 7 Select the report items to be generated in the left pane. You can preview the report items in the right pane. After confirming the report items, click **Save**, and enable security report subscription.

----End

9.4.3 Checking a Security Report

You can check **daily**, weekly, monthly, and **custom** reports, which are stored for six months. The reports show your server security trends and key security events and risks.

This section describes how to view the generated reports.

Security Report Overview

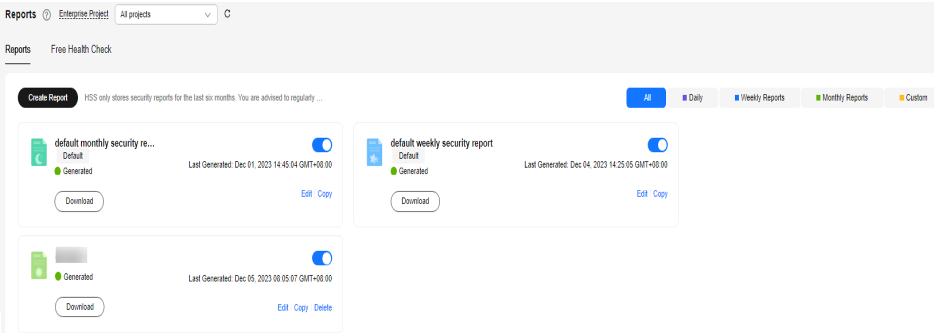
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Figure 9-19 Checking a security report



HSS only stores security reports for the last six months. You are advised to regularly ...

Last Generated: Dec 01, 2023 14:45:04 GMT+08:00

Last Generated: Dec 04, 2023 14:25:05 GMT+08:00

Last Generated: Dec 05, 2023 08:05:07 GMT+08:00

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click **Download** to go to the preview page. You can check the information of the target report and download or send it.

----End

Checking Report History

The report history stores the report sending details.

Step 1 In the upper right corner of the security report overview page, click **Report History** to check the report sending records.

Step 2 Check the report history on the displayed page, as shown in the following picture. For more information, see **Table 9-31**.

Table 9-31 Parameter description

Parameter	Description
Report Name	Name of a sent report.
Statistical Period	Statistical period of a sent report.
Report Type	Statistical period type of a sent report. ● Weekly Reports ● Monthly Reports ● Daily Reports ● Custom Reports
Sent	Time when the report is sent.

Step 3 Click **Download** in the **Operation** column to check historical reports. You can also preview and download the reports.

----End

9.4.4 Managing Security Reports

You can modify, cancel, or unsubscribe to a report.

Editing a Report

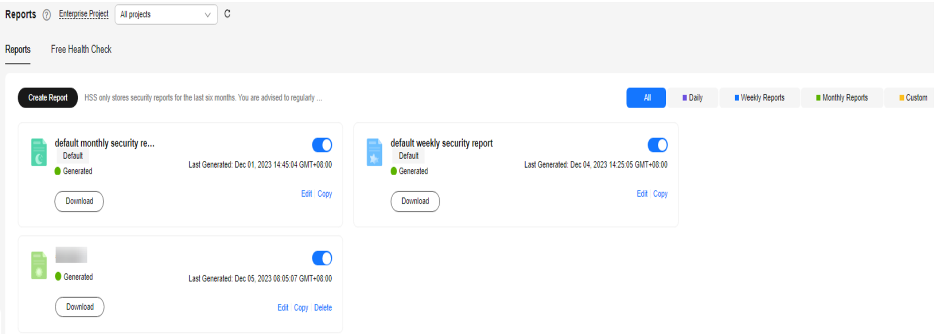
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Figure 9-20 Checking a security report



Reports | Enterprise Project: All projects

HSS only stores security reports for the last six months. You are advised to regularly ...

default monthly security re... — Default — Generated — Last Generated: Dec 01, 2023 14:45:04 GMT+08:00

default weekly security report — Default — Generated — Last Generated: Dec 04, 2023 14:25:05 GMT+08:00

[redacted] — Generated — Last Generated: Dec 05, 2023 08:05:07 GMT+08:00

Step 4 Click **Edit** in the lower right corner of the target report.

Step 5 Edit basic information of a report. For more information, see **Table 9-32**.

Table 9-32 Parameter description

Parameter	Description	Example Value
Report Name	Default report name.	**default monthly security report**
Report Type	Name of the statistical period type of a report, which cannot be edited.	**Monthly Reports**
Schedule Delivery	Time when a report is automatically sent.	-
Send Report To	Security report recipients. ● **Recipients specified in Message Center**: If you use Message Center settings, alarm notifications will be sent to the recipients specified in the **Security events** message type. You need to log in to the console and check the mailbox in the upper right corner. ● **Recipients specified in SMN topic**: If you use SMN topic settings, you can create a topic and specify recipients for HSS. ● **No need to send to email**: The report is not sent to the specified email address.	Recipients specified in SMN topic

Step 6 Confirm the information and click **Next** in the lower right corner of the page to configure the report.

Step 7 Select or deselect the report items in the pane on the left. You can preview the report items on the right. After confirming the report items, click **Save**. The report is changed successfully.

----End

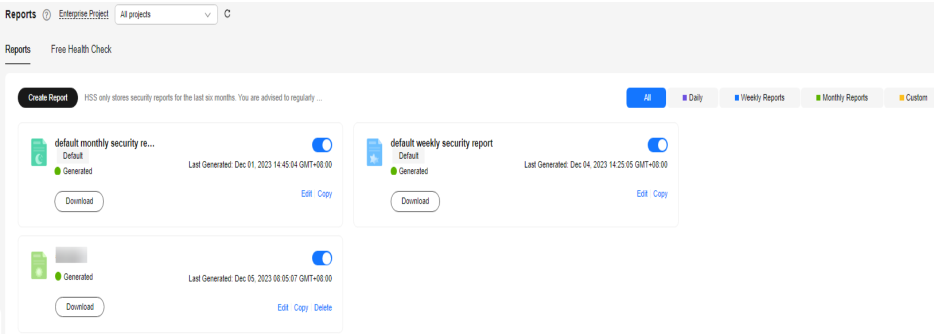
Enabling or Disabling Subscription

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Figure 9-21 Checking a security report



HSS only stores security reports for the last six months. You are advised to regularly ...

default monthly security re...
Default
Generated
Last Generated: Dec 01, 2023 14:45:04 GMT+08:00

default weekly security report
Default
Generated
Last Generated: Dec 04, 2023 14:25:05 GMT+08:00

Generated
Last Generated: Dec 05, 2023 08:05:07 GMT+08:00

Step 3 Click the switch in the upper right corner of a report to enable or disable the subscription.

- ◯: The subscription is disabled and no reports will be generated.
- ●: The subscription is enabled and reports will be generated on time.

----End

Deleting a Report

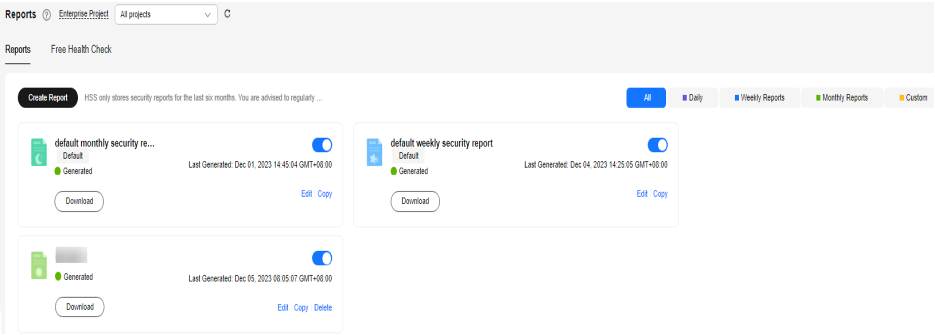
Default security report templates **default monthly security report** and **default weekly security report** cannot be deleted.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Security Operations** > **Reports**.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Figure 9-22 Checking a security report



HSS only stores security reports for the last six months. You are advised to regularly ...

default monthly security re...
Default
Generated
Last Generated: Dec 01, 2023 14:45:04 GMT+08:00

default weekly security report
Default
Generated
Last Generated: Dec 04, 2023 14:25:05 GMT+08:00

Generated
Last Generated: Dec 05, 2023 08:05:07 GMT+08:00

Step 3 Click **Delete** in the lower right corner of the target report.

----End

9.5 Free Health Check

HSS provides free health check for ECSs that are not protected by HSS, and for the CCE clusters where free health check is enabled. HSS generates security reports on the risks in servers and containers.

- Free server health check

  This function checks for the vulnerabilities, unsafe passwords, and asset risks on ECSs and generates reports.

  To enjoy advanced features like vulnerability management, baseline inspection, application protection, web tamper protection, ransomware protection, intrusion detection, file integrity management, and virus scanning, you can enable the professional edition or higher.

- Free container health check

  This function checks for image vulnerabilities, cluster configurations, privileged container risks and ports, and software information in CCE clusters, and generates reports.

  To enjoy advanced features like asset management, image security scanning, container firewall, and container cluster protection, enable the container edition.

Free Health Check

- ECSs that are not protected by HSS are scanned for free at 05:00 in the early morning on the first day of each month. (The time is subject to the time zone of the server.)
- To enable free health check for a CCE cluster, you can choose to enable security services when purchasing CCE or enable security services in the cluster configuration center. When you enable the free health check for the first time, HSS performs a health check immediately. Subsequent health checks are performed at 05:00 on the first day of each month.
- In a free server check 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.
- In a free container check report, up to five risk check results and 10 asset check results can be displayed.
- 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.
- You can purchase higher HSS editions to enjoy advanced functions, such as real-time protection, report download, online vulnerability fix, and compliance assistance.

Viewing the Free Health Checks of Servers

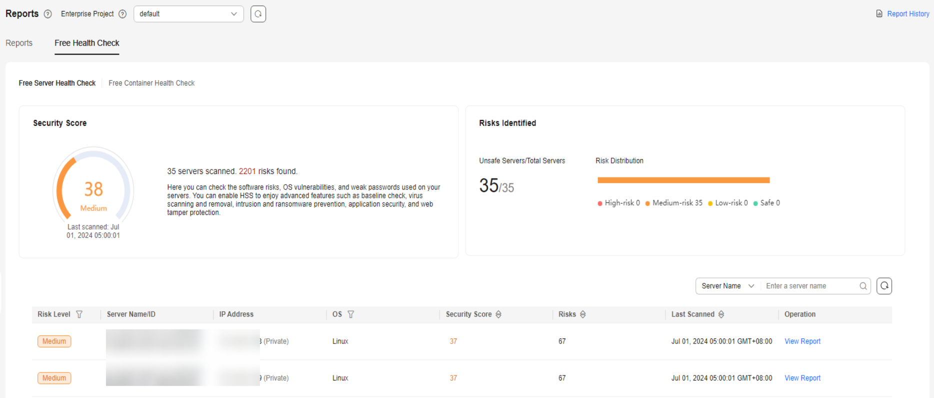
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane on the left, choose **Security Operations** > **Reports**.

Step 4 Click the **Free Health Check** tab and click **Free Server Health Check** to view the health check results of the servers that are not protected by HSS.

Figure 9-23 Viewing the free health check results of servers



Reports Enterprise Project default

Report History

Reports Free Health Check

Free Server Health Check Free Container Health Check

Security Score

38 Medium

Last scanned: Jul 01, 2024 05:00:01

35 servers scanned. 2201 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.

Risks Identified

Unsafe Servers/Total Servers: 35/35

Risk Distribution: ● High-risk 0 ● Medium-risk 35 ● Low-risk 0 ● Safe 0

Server Name | Enter a server name

Risk Level	Server Name/ID	IP Address	OS	Security Score	Risks	Last Scanned	Operation
Medium	[redacted]	[redacted] (Private)	Linux	37	67	Jul 01, 2024 05:00:01 GMT+08:00	View Report
Medium	[redacted]	[redacted] (Private)	Linux	37	67	Jul 01, 2024 05:00:01 GMT+08:00	View Report

Step 5 In the **Operation** column of a server, click **View Report** to view the health check report online.

----End

Viewing the Free Health Check Results of Containers

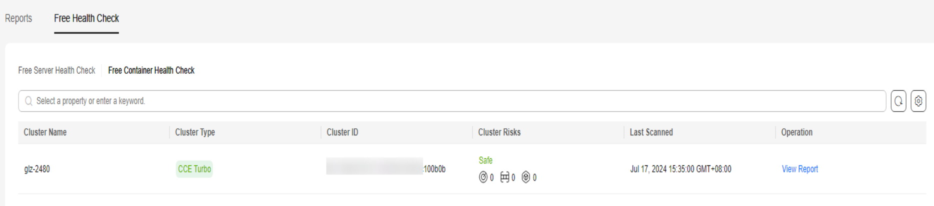
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Security Operations** > **Reports**.

Step 4 Click the **Free Health Check** tab and click **Free Container Health Check** to view the health check results of the container clusters that are not protected by HSS.

Figure 9-24 Viewing the free health check results of containers



Reports Free Health Check

Free Server Health Check Free Container Health Check

Select a property or enter a keyword.

Cluster Name	Cluster Type	Cluster ID	Cluster Risks	Last Scanned	Operation
glz-2480	CCE Turbo	[redacted]100b0b	Safe 0 0 0	Jul 17, 2024 15:35:00 GMT+08:00	View Report

Step 5 In the **Operation** column of a cluster, click **View Report** to view the health check report online.

----End

9.6 Monthly Operation Summary

On the first day of each month, HSS generates a security operations summary report for last month. You can learn the asset security status and security configurations, analyze past security operations, and harden configurations and improve O&M efficiency accordingly.

Constraints

- If you have not accessed HSS last month, no monthly operation summary report will be generated this month.
- The monthly operation summary report include statistics on all enterprise projects and cannot be generated for specific enterprise projects.
- Only the monthly operation summary reports of the latest 12 months are retained.

Checking a Monthly Operation Report

Step 1 Log in to the management console.

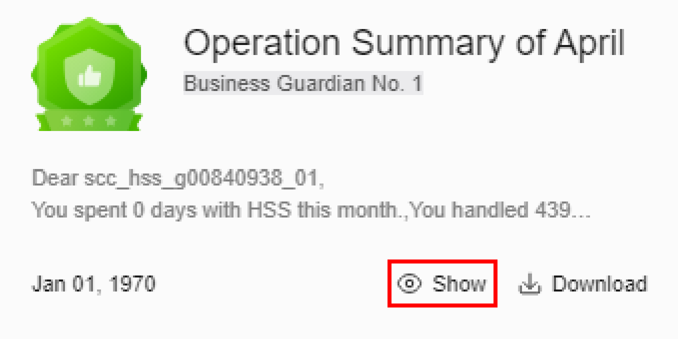
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the upper right corner of the **Dashboard** page, click **Operation Summary**.

Step 4 Click **Show** in a monthly report card.

To download a monthly operation summary report to your local PC, click **Download**. Open the **index.html** file in the downloaded package.

Figure 9-25 Checking a Monthly Operation Summary



Operation Summary of April

Business Guardian No. 1

Dear scc_hss_g00840938_01,
You spent 0 days with HSS this month.,You handled 439...

Jan 01, 1970

NOTE

On the first day of each month, a dialog box is displayed, prompting you to view the monthly operation summary. You can click **Learn More** to go to the summary page. If you select **Don't show again**, you can refer to the preceding procedure to view the summary later.

----End

10 Installation and Configuration on Servers

10.1 Agent Management

10.1.1 Agent Release Notes

HSS will be continuously optimized to improve service capabilities, including but not limited to adding functions and fixing defects. This document describes the updates in each version of the HSS agent.

Agent release notes (Linux)

Agent Version	Update Description
3.2.18	Added the local image application vulnerability scan to resolve known issues on the live network.
3.2.17	1. Emergency vulnerability scans support the Arm architecture. 2. Antivirus can scan TXT files in sensitive mode. 3. The ransomware honeypot module can check honeypot deployment failures. 4. Agent protection can be degraded. Known issues on the live network have been fixed.
3.2.15	The bugs of the container security edition were fixed. Known issues on the live network were resolved.
3.2.14	Fileless attack detection is supported. Known issues on the live network are resolved.
3.2.13	The agent can be installed using a key or password. The installation and configuration page is optimized. Known issues on the live network are resolved.

Agent Version	Update Description
3.2.12	1. The self-protection function is added to prevent malicious programs from stopping the HSS service process and uninstalling the service agent. 2. Container image scan supports the containerd runtime. 3. Baseline checks based on the HCE1.1 general security standard is supported. 4. Apache RocketMQ applications can be identified. Known issues on the live network were resolved.
3.2.11	Fixed the issue that container information occasionally fails to be collected.
3.2.10	1. Added automatic virus scan and removal. 2. IPv6 addresses are supported for each function module. 3. Added the port honeypot function. 4. Fixed known issues of the honeypot module on the live network.
3.2.9	1. Added the virus scan and removal function to support quick, full-disk, and custom scan and removal. Static files on disks can be scanned to enhance virus defense capabilities. 2. Added the antivirus detection function to check the files flushed to disks in real time and identify most known malicious programs. 3. Added the emergency vulnerability detection function to check for emergency vulnerabilities. 4. Fixed known issues on the live network.

Agent Release Notes (Windows)

Agent Version	Update Description
4.0.27	1. Added the function of killing processes in the kernel mode. 2. Added the AI ransomware detection function. 3. Added the source tracing function based on graph algorithms. 4. Fixed known issues on the live network.

Agent Version	Update Description
4.0.26	1. Emergency vulnerability scans are supported. 2. Antivirus can scan TXT files in sensitive mode. 3. The ransomware honeypot module can check driver installation failures honeypot deployment failures. 4. The ransomware intelligence database supports filtering. 5. Agent protection can be degraded. Known issues on the live network have been fixed.
4.0.25	Fixed known issues on the live network.
4.0.24	The agent can be installed through the GUI or script. The installation and configuration GUI was optimized. Known issues on the live network were resolved.
4.0.23	Known issues on the live network were resolved.
4.0.22	1. Added automatic virus scan and removal. 2. IPv6 addresses are supported for each function module. 3. Added the port honeypot function. 4. Fixed known issues of the honeypot module on the live network.
4.0.21	Fixed known issues on the live network.
4.0.20	1. Added the virus scan and removal function to support quick, full-disk, and custom scan and removal. Static files on disks can be scanned to enhance virus defense capabilities. 2. Added the common weak password detection function to check for weak passwords in Windows. 3. Fixed known issues on the live network.
4.0.19	1. Added the samples uploading function. 2. Added the application control (process whitelist) function. 3. Brute-force attack detection is supported for SQL Servers. 4. Added the SQL Server baseline check.

10.1.2 Viewing Agent Status

The HSS agent is a piece of software installed on cloud servers to exchange data between the servers and HSS, implementing security detection and protection. If no agent is installed, HSS is unavailable. For details about how to install the agent, see **Installing the Agent on Servers**.

This section describes how to view the agent status.

Viewing Agent Status

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**. Click the **Agents** tab.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Check the agent status and version of the server.

----End

10.1.3 Upgrading the Agent

HSS keeps improving its service capabilities, including but not limited to new features and defect fixes. Please upgrade your agent to the latest version in a timely manner to enjoy better service.

About the Upgrade

- Agent upgrade is free of charge.
- The upgrade does not affect the workloads on your cloud servers.
- You are advised to perform the upgrade during off-peak hours.
- If the agent has not been upgraded for more than six months, HSS will automatically upgrade it to the latest version. In the latest version, the known issues in earlier versions are fixed, and the threat detection and defense capabilities are enhanced to improve overall security. The upgrade is performed by HSS in the time window from 22:00 to 06:00 the next day. It does not affect your services.

Manually Upgrading the Agent

Step 1 Log in to the management console.

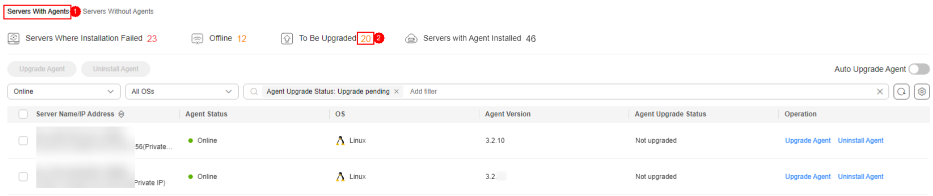
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**. The **Agents** page is displayed.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click the **Servers with Agents** tab and filter the servers where the agent needs to be upgraded.

Figure 10-1 Filtering servers where the agent needs to be upgraded



Server Name/IP Address	Agent Status	OS	Agent Version	Agent Upgrade Status	Operation
56(Private...	Online	Linux	3.2.10	Not upgraded	Upgrade Agent Uninstall Agent
Private IP)	Online	Linux	3.2.	Not upgraded	Upgrade Agent Uninstall Agent

Step 6 In the **Operation** column of a server, click **Upgrade Agent**.

You can also select target servers in batches and click **Upgrade Agent** in the upper left corner of the server list to upgrade agents for the servers in batches.

Step 7 In the displayed dialog box, confirm the server whose agent is to be upgraded and click **OK** to start the automatic upgrade.

Step 8 After the upgrade completes, check the agent version. If the latest version agent is used, the upgrade is successful.

----End

Automatically Upgrading Agents

Step 1 Log in to the management console.

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

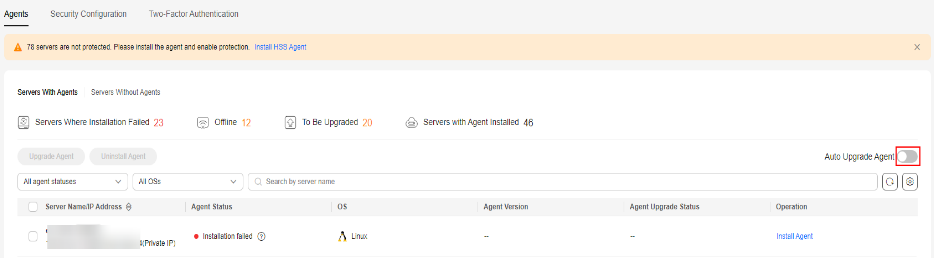
Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**. The agent management page is displayed.

Step 4 (Optional) If you have enabled the enterprise project function, select an enterprise project from the **Enterprise Project** drop-down list in the upper part of the page to view its data.

Step 5 Click ○ to enable automatic agent upgrade.

After this function is enabled, HSS checks the agent to be upgraded from 00:00 to 06:00 every day and automatically upgrades the agent to the latest version. The automatic upgrade can be performed only when the agent status is **Online**.

Figure 10-2 Enabling auto upgrade



78 servers are not protected. Please install the agent and enable protection.

Server Name/IP Address	Agent Status	OS	Agent Version	Agent Upgrade Status	Operation
(Private IP)	Installation failed	Linux	--	--	Install Agent

----End

Related Operations

For details about how to install an agent, see **Installing the Agent on Servers**.

10.1.4 Uninstalling the Agent

If you no longer need to use HSS, uninstall its agent from your servers. After the agent is uninstalled, HSS will not protect your servers or detect risks.

Uninstallation Methods

You can uninstall the agent in either of the following ways:

- One-click uninstallation: Uninstall the agent on the HSS console. For details, see **Uninstalling the Agent on the HSS Console**.
- Manual uninstallation: Uninstall the agent on the server. For details, see **Manually Uninstalling the Agent from a Server**.

You are advised to uninstall the agent in one-click mode, simple and efficient. If the agent is in **Offline** state and cannot be uninstalled on the HSS console, you can manually uninstall it.

Uninstalling the Agent on the HSS Console

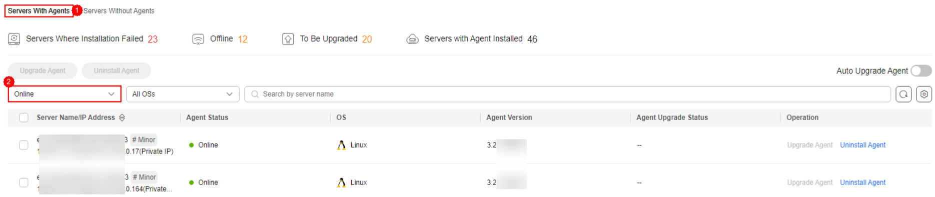
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Server Install & Config**. Click the **Agents** tab.

Step 4 Click the **Servers with Agents** tab and filter the servers with online agents.

Figure 10-3 Filtering servers with online agents



Servers With Agents 1 Servers Without Agents

Servers Where Installation Failed 23 Offline 12 To Be Upgraded 20 Servers with Agent Installed 46

Upgrade Agent Uninstall Agent Auto Upgrade Agent

2 Online All OSs Search by server name

□ Server Name/IP Address	Agent Status	OS	Agent Version	Agent Upgrade Status	Operation

□ [redacted] 3 # Minor
0.17(Private IP)
	● Online	Linux	3.2 [redacted]	--	Upgrade Agent Uninstall Agent

□ [redacted] 3 # Minor 0.164(Private...	● Online	Linux	3.2 [redacted]	--	Upgrade Agent Uninstall Agent

Step 5 Click **Uninstall Agent** in the **Operation** column of a server. In the dialog box that is displayed, confirm the uninstallation information and click **OK**.

If you need to uninstall the agent in batches, you can select servers and click **Uninstall Agent** above the list.

Step 6 Wait for about 5 to 10 minutes. Click the **Servers Without Agents** tab and find the target server. If the agent status of the target server is **Uninstalled**, the agent has been uninstalled.

----End

Manually Uninstalling the Agent from a Server

- **Uninstalling the Linux agent**

  a. Log in to the server from which you want to uninstall the agent and run the following command to switch to user root:

     su - root

  b. Perform the following operations to stop HSS:

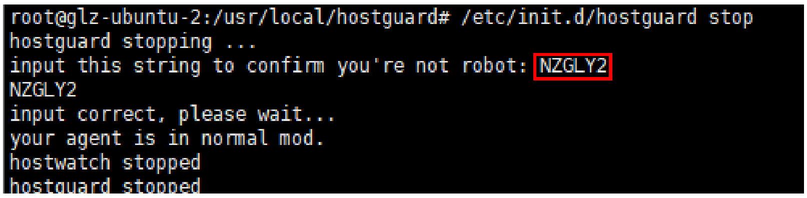
     i. Run the following command to stop the service:

        /etc/init.d/hostguard stop

     ii. (Optional) Enter the verification code displayed in the command output. See **Figure 10-4**.

        This operation is required only for servers where HSS self-protection is enabled.

        Figure 10-4 Verification code



```
root@glz-ubuntu-2:/usr/local/hostguard# /etc/init.d/hostguard stop
hostguard stopping ...
input this string to confirm you're not robot: NZGLY2
NZGLY2
input correct, please wait...
your agent is in normal mod.
hostwatch stopped
hostguard stopped
```

  c. In any directory, run the following command to uninstall the agent:

     Do not run the uninstallation command in the **/usr/local/hostguard/** directory. You can run the uninstallation command in any other directory.

     - For EulerOS, CentOS and Red Hat, or other OSs that support RPM installation, run the **rpm -e hostguard** command.

     - For Ubuntu and Debian OSs, or other OSs that support DEB installation, run the **dpkg -P hostguard** command.

     If the information similar to the following is displayed, the agent has been uninstalled. No further action is required. Wait for about 15 minutes. The agent status of the server on the HSS console will change to **Uninstalled** or **Offline**. If the uninstallation fails, go to the **d**.

```
Stopping Hostguard...
Hostguard stopped
Hostguard uninstalled.
```

  d. (Optional) If the agent fails to be uninstalled in **c**, perform the following operations to uninstall the agent:

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

       1) Run the following command to delete the installation record:

          rpm -e --justdb hostguard

       2) Run the following command to check whether there are hostguard processes:

          ps -ef | grep hostguard

          If there are residual processes, run the **kill -9 PID** command to stop all residual processes.

3) Run the following command to check whether the **/usr/local/hostguard** directory exists:

   ll /usr/local/hostguard

   If the directory exists, run the **rm -rf /usr/local/hostguard** command to delete it.

4) Run the following command to check whether the **/etc/init.d/hostguard** file exists:

   ll /etc/init.d/hostguard

   If the file exists, run the **rm -f /etc/init.d/hostguard** command to delete the file.

- For OSs that support DEB installation, such as Ubuntu and Debian:

  1) Run the following command to check whether there are hostguard processes:

     ps -ef | grep hostguard

     If there are residual processes, run the **kill -9 PID** command to stop all residual processes.

  2) Run the following command to check whether the **/usr/local/hostguard** directory exists:

     ll /usr/local/hostguard

     If the directory exists, run the **rm -rf /usr/local/hostguard** command to delete it.

  3) Run the following command to check whether the **/etc/init.d/hostguard** file exists:

     ll /etc/init.d/hostguard

     If the file exists, run the **rm -f /etc/init.d/hostguard** command to delete the file.

- **Uninstalling the Windows agent**

  a. (Optional) Disable HSS self-protection.

     If HSS self-protection is enabled, disable it and then uninstall the agent. Otherwise, the agent cannot be uninstalled locally on the server. For details about how to disable the function, see **How Do I Disable the Agent Self-protection Policy?**

  b. Log in to the server that you want to uninstall the agent.

  c. Click **Start** and choose **Control Panel** > **Programs**. Then select **HostGuard** and click **Uninstall**.

     NOTE

     - Alternatively, go to the **C:\Program File\HostGuard** directory and double-click **unins000.exe** to uninstall the program.
     - If you have created a folder for storing the agent shortcut under the **Start** menu when installing the agent, you can also choose **Start** > **HostGuard** > **Uninstall HostGuard** to uninstall HostGuard.

  d. In the **Uninstall HostGuard** dialog box, click **Yes**.

  e. (Optional) Restart the server.

- If you have enabled WTP, you need to restart the server after uninstalling the agent. In the **Uninstall HostGuard** dialog box, click **Yes** to restart the server.
- If you have not enabled WTP, you do not need to restart the server. In the **Uninstall HostGuard** dialog box, click **No** to skip server restart.

Related Operations

Installing the Agent on Servers

11 Installation and Configuration on Containers

11.1 Installing an Agent in a Cluster

11.1.1 Overview of Agent Installation in a Cluster

HSS can protect Huawei Cloud CCE clusters, third-party cloud clusters, and on-premises clusters. This section describes how to install an agent for these assets.

Context

In earlier versions, HSS provides **cluster agent management** to connect to containers. However, the containers connected in this way cannot use some container-related functions, such as container firewall and container cluster protection.

To solve this problem, in Linux agent 3.2.12 or later and Windows agent 4.0.23 or later, HSS supports **installation and configuration management on containers** to replace **cluster agent management**. Using the new function, cluster assets can fully connect to HSS and enjoy all the container-related functions provided.

If you have connected HSS to your cluster assets through **cluster agent management**, you are advised to uninstall the agent from your clusters, and then connect to them again by following the instructions provided in this section. In this way, you can fully enjoy cluster security functions. For more information, see **Uninstalling the Agent from a Cluster**.

Notice on ANP-Agent

ANP-Agent is different from HSS Agent. When the HSS agent is installed in a **non-CCE** cluster, ANP-Agent is used to enable the communication between HSS and the cluster. For details about the HSS agent, see **Agent Overview**.

Installing an Agent

The procedure for installing the agent varies depending on the cluster type. For details, see the following:

- **Installing the Agent in a Huawei Cloud CCE Cluster**
- **Installing an Agent in a User-built Cluster on Huawei Cloud**
- **Installing the Agent in a Third-Party Public Network Cluster**
- **Installing the Agent in a Third-Party Private Network Cluster**

11.1.2 Installing the Agent in a Huawei Cloud CCE Cluster

Scenario

Install the agent in a Huawei Cloud CCE cluster. After the configuration is complete, HSS automatically installs the agent on existing cluster nodes, installs the agent on new nodes when the cluster is scaled out, and uninstalls the agent from removed nodes when the cluster is scaled in.

Prerequisites

Before installing an agent for a CCE cluster, grant the CCEOperatePolicy permission to HSS. For details, see **Authorization**.

Constraints

- Supported container runtime: Docker and Containerd
- Supported cluster editions: CCE standard and Turbo editions
- Node resource requirements: At least 50 MiB memory and 200m CPU should be available.
- When an agent is installed in a cluster, HSS creates an HSS namespace in the cluster.

Installing the Agent in a Huawei Cloud CCE Cluster

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

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 On the **Cluster** tab page, click **Install Container Agent**. The **Container Asset Access and Installation** slide-out panel is displayed.

Step 5 Select **CCE Cluster Installation** and click **Configure Now**.

Step 6 Select a cluster and click **Next**.

Step 7 Configure agent parameters. For more information, see **Table 11-1**.

Table 11-1 Agent parameters

Parameter	Description
Configuration Rules	Select an agent configuration rule. ● **Default Rule**: Select this if the sock address of container runtime is a common address. The agent will be installed on nodes having no taints. ● **Custom**: Select this rule if the sock address of your container runtime is not a common address or needs to be modified, or if you only want to install the agent on specific nodes. **NOTE** ● If the sock address of your container runtime is incorrect, some HSS functions may be unavailable after the cluster is connected to HSS. ● You are advised to select all runtime types.
(Optional) Advanced Configuration	This parameter can be set if **Custom** is selected for **Configuration Rules**. Click ˅ to expand advanced configurations. The **Enabling auto upgrade agent** option is selected by default. ● **Enabling auto upgrade** Configure whether to enable automatic agent upgrade. If it is enabled, HSS automatically upgrades the agent to the latest version between 00:00 to 06:00 every day to provide you with better services. ● **Node Selector Configuration** Set the **Key** and **Value** of tags of the nodes where the agent is to be installed and click **Add**. If no tags are specified, the agent will be installed on all the nodes having no taints. ● **Tolerance Configuration** If you added a node whose tag contains a taint in **Node Selector Configuration**, set the **Key**, **Value**, and **Effect** of the taint, and click **Add** to allow agent installation on the node.

Step 8 Click **OK** to start installing the HSS agent.

Step 9 In the cluster list, check the cluster status. If the cluster status is **Running**, the cluster is successfully connected to HSS.

----End

Follow-up Procedure

After the agent is installed in a cluster, enable protection.

11.1.3 Installing an Agent in a User-built Cluster on Huawei Cloud

Scenario

Install the agent on a user-built cluster on Huawei Cloud that can access the SWR image repository. After the configuration is complete, HSS automatically installs the agent on existing cluster nodes, installs the agent on new nodes when the cluster is scaled out, and uninstalls the agent from removed nodes when the cluster is scaled in.

Step 1: Prepare the kubeconfig File

The kubeconfig file specifies the cluster permissions assigned to HSS. The kubeconfig file configured using method 1 contains the cluster administrator permissions, whereas the file generated using method 2 contains only the permissions required by HSS. If you want to minimize HSS permissions, prepare the file using method 2.

- **Method 1: configuring the default kubeconfig file**

  a. Perform the following operations to create a dedicated namespace for HSS:

  i. Log in to a cluster node.

  ii. Create the **hss.yaml** file and copy the following content to the file:

  ```
  {"metadata":{"name":"hss"},"apiVersion":"v1","kind":"Namespace"}
  ```

  iii. Run the following command to create a namespace:

  ```
  kubectl apply -f hss.yaml
  ```

  b. Find and download the **config** file in the **$HOME/.kube/config** directory.

  c. Change the file name from **config** to **config.yaml**.

- **Method 2: generating a kubeconfig file dedicated to HSS**

  a. Create a dedicated namespace and an account for HSS.

  i. Log in to a cluster node.

  ii. Create the **hss-account.yaml** file and copy the following content to the file:

  ```
  {"metadata":{"name":"hss"},"apiVersion":"v1","kind":"Namespace"}{"metadata":
  {"name":"hss-user","namespace":"hss"},"apiVersion":"v1","kind":"ServiceAccount"}
  {"metadata":{"name":"hss-user-token","namespace":"hss","annotations":{"kubernetes.io/
  service-account.name":"hss-user"}},"apiVersion":"v1","kind":"Secret","type":"kubernetes.io/
  service-account-token"}
  ```

  iii. Run the following command to create a namespace and an account:

  ```
  kubectl apply -f hss-account.yaml
  ```

  b. Generate the kubeconfig file.

  i. Create the **gen_kubeconfig.sh** file and copy the following content to the file:

  ```
  #!/bin/bash

  KUBE_APISERVER=`kubectl config view  --output=jsonpath='{.clusters[].cluster.server}' |
  head -n1 `
  CLUSTER_NAME=`kubectl config view -o jsonpath='{.clusters[0].name}'`
  kubectl get secret hss-user-token -n hss -o yaml |grep ca.crt: | awk '{print $2}' |base64 -d
  >hss_ca_crt
  ```

```
kubectl config set-cluster ${CLUSTER_NAME} --server=${KUBE_APISERVER}  --certificate-authority=hss_ca_crt  --embed-certs=true --kubeconfig=hss_kubeconfig.yaml
kubectl config set-credentials hss-user --token=$(kubectl describe secret hss-user-token -n hss | awk '/token:/{print $2}') --kubeconfig=hss_kubeconfig.yaml
kubectl config set-context hss-user@kubernetes --cluster=${CLUSTER_NAME} --user=hss-user --kubeconfig=hss_kubeconfig.yaml
kubectl config use-context hss-user@kubernetes --kubeconfig=hss_kubeconfig.yaml
```

ii. Run the following command to generate the kubeconfig file named **hss_kubeconfig.yaml**:

```
bash gen_kubeconfig.sh
```

Step 2: Install an Agent in a User-built Cluster on Huawei Cloud

Step 1 Log in to the management console.

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

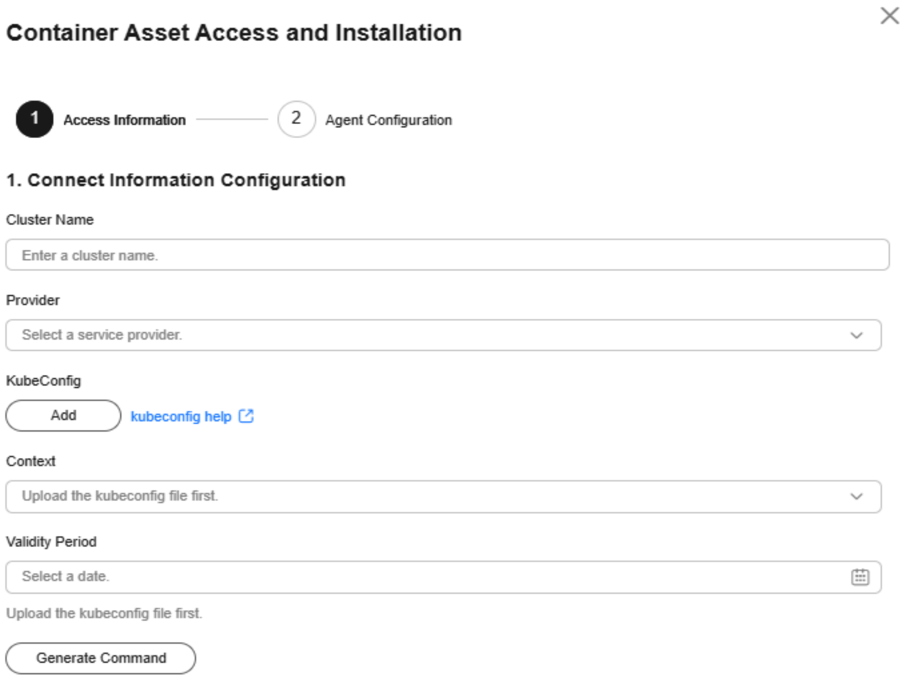
Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 On the **Cluster** tab page, click **Install Container Agent**. The **Container Asset Access and Installation** slide-out panel is displayed.

Step 5 Select **Non-CCE cluster (Internet access)** and click **Configure Now**.

Step 6 Configure cluster access information and click **Generate Command**. For more information, see **Table 11-2**.

Figure 11-1 Configuring cluster access information



Container Asset Access and Installation

1 Access Information — 2 Agent Configuration

1. Connect Information Configuration

Cluster Name: Enter a cluster name.

Provider: Select a service provider.

KubeConfig: Add   kubeconfig help

Context: Upload the kubeconfig file first.

Validity Period: Select a date.

Upload the kubeconfig file first.

Generate Command

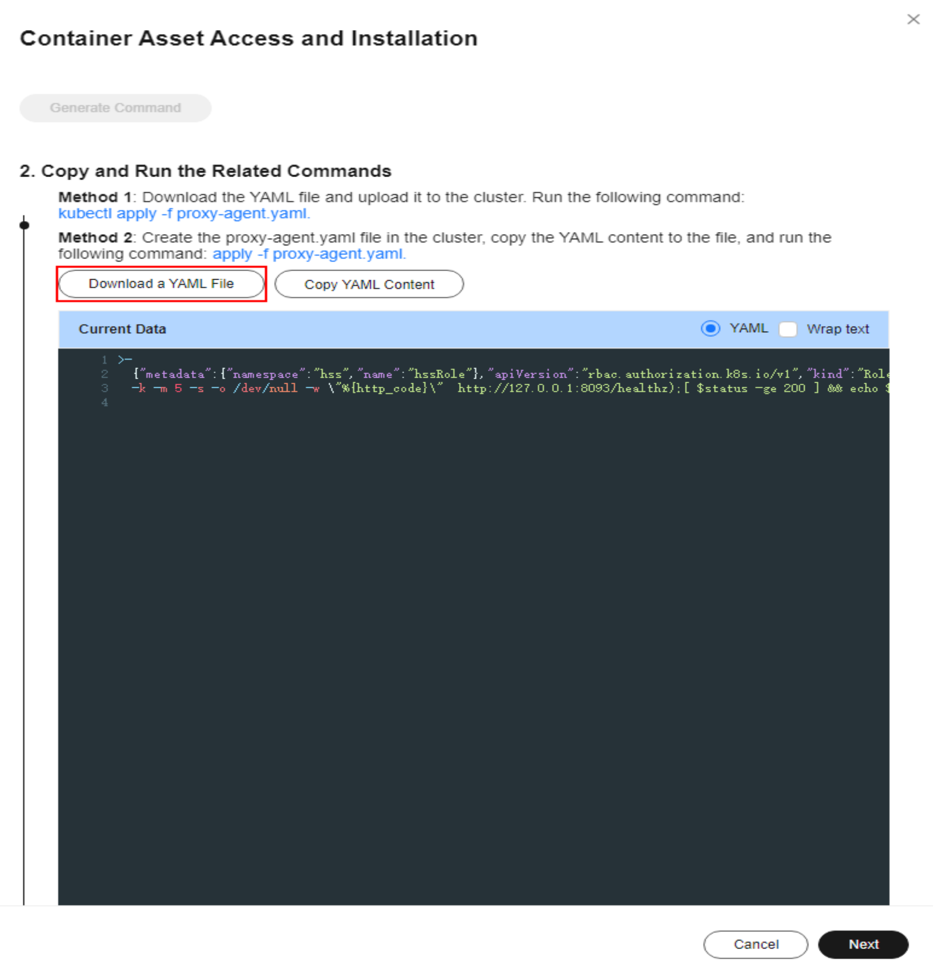
Table 11-2 Access parameters

Parameter	Description
Cluster Name	Name of the cluster to be connected.
Provider	Service provider of the cluster. Currently, the clusters of the following service providers are supported: ● Alibaba Cloud ● Tencent Cloud ● AWS ● Azure ● User-built ● On-premises IDC
KubeConfig	Add and upload the kubeconfig file configured as required in **Step 1: Prepare the kubeconfig File**.
Context	After the kubeconfig file is uploaded, HSS automatically parses the context.
Validity Period	After the kubeconfig file is uploaded, HSS automatically parses the validity period. You can also specify a time before the final validity period. After the specified validity period expires, you need to connect to the asset again.

Step 7 Perform the following operations to install the cluster connection component (ANP-agent) and establish a connection between HSS and the cluster:

1. In the **Container Asset Access and Installation** dialog box, click **Download a YAML File**.

Figure 11-2 Downloading the YAML file



Container Asset Access and Installation

2. Copy and Run the Related Commands

Method 1: Download the YAML file and upload it to the cluster. Run the following command: kubectl apply -f proxy-agent.yaml.

Method 2: Create the proxy-agent.yaml file in the cluster, copy the YAML content to the file, and run the following command: apply -f proxy-agent.yaml.

```
>-
  {"metadata":{"namespace":"hss","name":"hssRole"},"apiVersion":"rbac.authorization.k8s.io/v1","kind":"Rol
  -k -m 5 -s -o /dev/null -w \"%{http_code}\"  http://127.0.0.1:8093/healthz);[ $status -ge 200 ] && echo $
```

2. Copy the command file to a directory on any node.
3. Run the following command to install the cluster connection component (ANP-Agent):

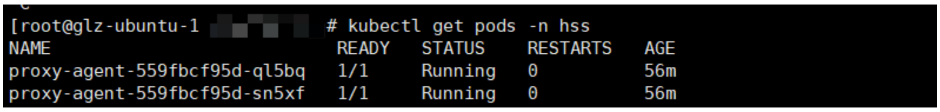
```
kubectl apply -f proxy-agent.yaml
```

4. Run the following command to check whether the cluster connection component (ANP-agent) is successfully installed:

```
kubectl get pods -n hss | grep proxy-agent
```

   If the command output shown in **Figure 11-3** is displayed, the cluster connection component (ANP-agent) is successfully installed.

Figure 11-3 ANP-Agent installed



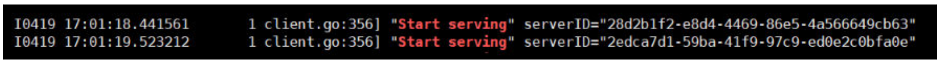
```
[root@glz-ubuntu-1 [redacted]  # kubectl get pods -n hss
NAME                          READY   STATUS    RESTARTS   AGE
proxy-agent-559fbcf95d-ql5bq  1/1     Running   0          56m
proxy-agent-559fbcf95d-sn5xf  1/1     Running   0          56m
```

5. Run the following command to check whether the cluster is connected to HSS:

```
for a in $(kubectl get pods -n hss| grep proxy-agent | cut -d ' ' -f1); do kubectl -n hss logs $a | grep 'Start serving';done
```

   If the command output shown in **Figure 11-4** is displayed, the cluster is connected to HSS.

Figure 11-4 Cluster connected to HSS



```
I0419 17:01:18.441561       1 client.go:356] "Start serving" serverID="28d2b1f2-e8d4-4469-86e5-4a566649cb63"
I0419 17:01:19.523212       1 client.go:356] "Start serving" serverID="2edca7d1-59ba-41f9-97c9-ed0e2c0bfa0e"
```

Step 8 In the **Container Asset Access and Installation** dialog box, click **Next**.

Step 9 Configure agent parameters. For more information, see **Table 11-3**.

Table 11-3 Agent parameters

Parameter	Description
Configuration Rules	Select an agent configuration rule. ● **Default Rule**: Select this if the sock address of container runtime is a common address. The agent will be installed on nodes having no taints. ● **Custom**: Select this rule if the sock address of your container runtime is not a common address or needs to be modified, or if you only want to install the agent on specific nodes. **NOTE** ● If the sock address of your container runtime is incorrect, some HSS functions may be unavailable after the cluster is connected to HSS. ● You are advised to select all runtime types.
(Optional) Advanced Configuration	This parameter can be set if **Custom** is selected for **Configuration Rules**. Click ⌄ to expand advanced configurations. The **Enabling auto upgrade agent** option is selected by default. ● **Enabling auto upgrade** Configure whether to enable automatic agent upgrade. If it is enabled, HSS automatically upgrades the agent to the latest version between 00:00 to 06:00 every day to provide you with better services. ● **Node Selector Configuration** Set the **Key** and **Value** of tags of the nodes where the agent is to be installed and click **Add**. If no tags are specified, the agent will be installed on all the nodes having no taints. ● **Tolerance Configuration** If you added a node whose tag contains a taint in **Node Selector Configuration**, set the **Key**, **Value**, and **Effect** of the taint, and click **Add** to allow agent installation on the node.

Step 10 Click **OK** to start installing the HSS agent.

Step 11 In the cluster list, check the cluster status. If the cluster status is **Running**, the cluster is successfully connected to HSS.

----End

Follow-up Procedure

After the agent is installed in a cluster, **enable protection**.

11.1.4 Installing the Agent in a Third-Party Public Network Cluster

Scenario

Install the agent on a third-party cluster that can access the public network. After the configuration is complete, HSS automatically installs the agent on existing cluster nodes, installs the agent on new nodes when the cluster is scaled out, and uninstalls the agent from removed nodes when the cluster is scaled in.

Constraints

- Supported cluster orchestration platforms: Kubernetes 1.19 or later
- Supported node OS: Linux
- Node specifications: at least 2 vCPUs, 4 GiB memory, 40 GiB system disk, and 100 GiB data disk
- The agent is incompatible with clusters of Galera 3.34, MySQL 5.6.51, or earlier versions.

Step 1: Create a VPC

Step 1 Log in to the console and go to the page for **Creating a VPC**.

Step 2 On the **Create VPC** page, set parameters for the VPC and subnets as prompted.

You are advised to set some parameters by referring to **Table 11-4** and retain the default values for other parameters. For details about how to create a VPC, see **Creating a VPC**.

Table 11-4 Parameters for creating a VPC

Parameter	Description	Example Value
Region	Select a region near you to ensure the lowest latency possible.	CN-Hong Kong
Name	VPC name. The name: ● Must contain 1 to 64 characters. ● Can contain letters, numbers, underscores (_), hyphens (-), and periods (.).	HSS-outside-anp-VPC

Parameter	Description	Example Value
Enterprise Project	Enterprise project to which the VPC belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.	default
Subnet Name	Subnet name. The name: ● Must contain 1 to 64 characters. ● Can contain letters, numbers, underscores (_), hyphens (-), and periods (.).	HSS-outside-subnet

Step 3 Click **Create Now**. You can view the VPC after it is created.

----End

Step 2: Create a Security Group

Step 1 In the navigation pane on the left, choose **Access Control** > **Security Groups**.

Step 2 Click **Create Security Group** in the upper right corner.

Step 3 Configure security group parameters as prompted.

You are advised to configure some parameters by referring to **Table 11-5** and configure other parameters based on site requirements. For details about how to create a security group, see **Creating a Security Group**.

Table 11-5 Parameters for creating a security group

Parameter	Description	Example Value
Region	Select a region near you to ensure the lowest latency possible.	CN-Hong Kong
Name	Specify the name of the security group. The name: ● Must contain 1 to 64 characters. ● Can contain letters, numbers, underscores (_), hyphens (-), and periods (.).	HSS-outside-anp-secGroups

Parameter	Description	Example Value
Enterprise Project	When creating a security group, you can add the security group to an enterprise project that has been enabled. An enterprise project facilitates project-level management and grouping of cloud resources and users. The default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.	default
Preset Rule	Inbound and outbound rules are preset in security group rules. You can select a rule as needed to quickly create a security group.	All ports open

Step 4 Click **Create Now**. You can view the security group after it is created.

----End

Step 3: Create an ECS

Step 1 Click ☰ in the upper left corner and **Compute** > **Elastic Cloud Server**.

Step 2 In the upper right corner, click **Buy ECS**.

Step 3 Configure ECS parameters as prompted.

You are advised to configure some parameters by referring to **Table 11-6** and configure other parameters based on site requirements.

Table 11-6 Parameters for purchasing an ECS

Parameter	Description	Example Value
Billing Mode	ECS billing mode. ● Yearly/Monthly: Prepaid mode. Yearly/monthly ECSs are billed by the purchased duration specified in the order. ● Pay-per-use: Postpaid billing mode. You pay as you go and just pay for what you use. Pay-per-use ECSs are billed by the second and settled by the hour. ● Spot price: Spot pricing is a postpaid billing mode. You pay as you go and just pay for what you use. In **Spot pricing** billing mode, your purchased ECS is billed at a lower price than that of a pay-per-use ECS with the same specifications. In **Spot pricing** billing mode, you can select **Spot** or **Spot block** for the **Spot Type**. Spot ECSs and Spot block ECSs are billed by the second and settled by the hour.	Pay-per-use
Region	Select a region near you to ensure the lowest latency possible.	CN-Hong Kong
CPU Architecture	Select a CPU architecture. The value can be **x86**.	x86
Instance	● Select vCPUs and memory, or enter a keyword to search for ECS specifications. You can search for ECS flavors when you select **By Type**. ● Select ECS specifications by instance family and generation from the list.	General computing, 2 vCPUs, 4 GiB
Image	An image is an ECS template that contains an OS. It may also contain proprietary software and application software. You can use images to create ECSs.	Public image, EulerOS 2 5 64bit (40 GiB)
System Disk	A system disk stores the OS of an ECS, and is automatically created and initialized upon ECS creation.	Ultra-high I/O
Network	VPC allows you to create logically isolated, configurable, and manageable virtual networks for VPCs. You can configure security groups, Virtual Private Network (VPNs), CIDR blocks, and bandwidths in your VPC. ECSs in different VPCs cannot communicate with each other by default.	HSS-outside-anp-VPC (VPC created in **Step 1: Create a VPC**)

Parameter	Description	Example Value
Security Group	Select an available security group from the drop-down list. You can select multiple security groups for an ECS (no more than five security groups are recommended). The access rules of all the selected security groups apply to the ECS.	HSS-outside-anp-secGroups (Security group created in **Step 2: Create a Security Group**)
EIP	An EIP is a static public IP address bound to a cloud server in a VPC. Using the EIP, the cloud server provides services externally.	Buy now, static BGP
ECS Name	This parameter will be set to the initial server name (**hostname**) in the ECS OS. The name can contain only letters, numbers, underscores (_), hyphens (-), and periods (.).	HSS-outside-anp-ECS
Enterprise Project	When purchasing an ECS, you can add it to an enabled enterprise project. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.	default
Login Mode	Method for logging in to an ECS.	Password

Step 4 Click **Create**. In the displayed dialog box, click **Agree and Create**. After the payment is complete, the ECS will be automatically created and started by default.

----End

Step 4: Set Up Nginx

Step 1 Log in to the server created in **Step 3: Create an ECS**.

Step 2 Go to the **temp** directory.

cd /temp

Step 3 Run the following command to create the **install_nginx.sh** file:

vi install_nginx.sh

Step 4 Press **i** to enter the editing mode and copy the following content to the **install_nginx.sh** file:

```
#!/bin/bash

yum -y install pcre-devel zlib-devel popt-devel openssl-devel openssl
```

```
wget http://www.nginx.org/download/nginx-1.21.0.tar.gz
tar zxf nginx-1.21.0.tar.gz -C /usr/src/
cd /usr/src/nginx-1.21.0/
useradd -M -s /sbin/nologin nginx
./configure \
--prefix=/usr/local/nginx \
--user=nginx \
--group=nginx \
--with-file-aio \
--with-http_stub_status_module \
--with-http_gzip_static_module \
--with-http_flv_module \
--with-http_ssl_module \
--with-stream \
--with-pcre && make && make install
ln -s /usr/local/nginx/sbin/nginx /usr/local/sbin/
nginx
```

Step 5 Enter **ECS**, run the following command, and press **Enter** to exit.

:wq!

Step 6 Run the following command to install Nginx:

bash /temp/install_nginx.sh

Step 7 Run the following command to modify the Nginx configuration file:

```
cat <<END >> /usr/local/nginx/conf/nginx.conf
stream {
  upstream backend_hss_anp {
    server {{ANP_proxy_address}}:8091 weight=5 max_fails=3 fail_timeout=30s;
  }
  server {
    listen 8091 so_keepalive=on;
    proxy_connect_timeout 10s;
    proxy_timeout 300s;
    proxy_pass backend_hss_anp ;
  }
}
END
```

Replace **{{ANP_proxy_address}}** with the actual address and then run the command. For details, see **Table 11-7**.

Table 11-7 ANP proxy address

Region	ANP proxy address
Guiyang1, Bangkok, Shanghai2, Guangzhou, Beijing4, Beijing2, and Shanghai1	hss-proxy.RegionCode.myhuaweicloud.com
Other	hss-anp.RegionCode.myhuaweicloud.com
For details about region codes, see **Regions and Endpoints**.	

Step 8 Run the following command to make the Nginx configuration take effect:

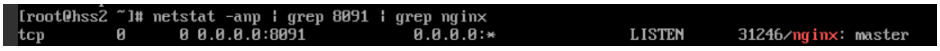
nginx -s reload

Step 9 Run the following command to check whether port 8091 is listened on properly:

netstat -anp | grep 8091

If information similar to **Figure 11-5** is displayed, the listening is normal.

Figure 11-5 Listening on port 8091 is normal.



```
[root@hss2 ~]# netstat -anp | grep 8091 | grep nginx
tcp        0      0 0.0.0.0:8091            0.0.0.0:*               LISTEN      31246/nginx: master
```

----End

Step 5: Buy and Configure an ELB

Step 1 Log in to the console and go to the page for **Buying ELB** page.

Step 2 Set ELB parameters as prompted.

You are advised to configure some parameters by referring to **Table 11-8** and configure other parameters based on site requirements. For details about how to buy a load balancer, see **Creating a Dedicated Load Balancer**.

Table 11-8 Parameters for buying an ELB

Parameter	Description	Example Value
Type	Type of the shared load balancer. The type cannot be changed after the load balancer is created. Dedicated load balancers work well for heavy-traffic and high-concurrency workloads, such as large websites, cloud native applications, IoV, and multi-AZ disaster recovery applications.	Dedicated
Billing Mode	Billing mode of a dedicated load balancer. ● **Yearly/Monthly**: prepaid billing mode. You pay in advance for a subscription term, and in exchange, you get a discounted rate. ● **Pay-per-use**: postpaid billing mode. You pay as you go and just pay for what you use. The load balancer usage is calculated by the second but billed every hour.	Pay-per-use
Region	Select a region near you to ensure the lowest latency possible.	CN-Hong Kong
Name	Load balancer name. The name can contain: ● 1 to 64 characters. ● Letters, numbers, underscores (_), hyphens (-), and periods (.).	HSS-outside-anp-ELB

Parameter	Description	Example Value
Enterprise Project	When creating a load balancer, you can add it to an enabled enterprise project. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.	default
Specification Type	Select **Elastic** or **Fixed** if pay-per-use is chosen as the billing mode. Specifications: ● Elastic specifications work well for fluctuating traffic, and you will be charged for how many LCUs you use. ● Fixed specifications are suitable for stable traffic, and you will be charged for the specifications you select.	● Fixed ● Network load balancing ● Small
Network Configuration	● **Network Type**: You can select one or more network types. – **Private IPv4 network**: The load balancer routes IPv4 requests from the clients to backend servers in a VPC. If you want the load balancer to route IPv4 requests from the Internet, bind an EIP to the load balancer. – **IPv6 network**: An IPv6 address will be assigned to the load balancer to route requests from IPv6 clients. ● **VPC**: VPC where the dedicated load balancer works. You cannot change the VPC after the load balancer is created. Plan the VPC as required. Select an existing VPC, or click **View VPCs** to create a desired one. ● **Frontend Subnet**: Subnet where the dedicated load balancer is located. The system allocates an IP address from this subnet to the load balancer for external services. After a load balancer is created, you can unbind the IP address from it and assign an IP address from a new frontend subnet to the load balancer. ● **Backend Subnet**: The load balancer uses IP addresses in the backend subnet to establish connections with backend servers.	● Private IPv4 network ● HSS-outside-anp-VPC (VPC created in **Step 1: Create a VPC**) ● HSS-outside-subnet (VPC subnet created in **Step 1: Create a VPC**) ● Subnet of the load balancer

Parameter	Description	Example Value
Elastic IPs	EIP that will be bound to the load balancer for receiving and forwarding IPv4 requests over the Internet.	● Auto assign ● Dynamic BGP ● Bandwidth

Step 3 After setting the parameters, click **Next**.

Step 4 On the ELB page, view the created ELB and record the public IPv4 address.

Step 5 In the row of a load balancer, click **Add now** in the **Listener (Frontend Protocol/ Port)** column.

Step 6 Set the listener parameters as prompted.

You are advised to configure some parameters by referring to **Table 11-9** and configure other parameters based on site requirements. For details, see **Adding a TCP Listener**.

Table 11-9 Parameters for adding a listener

Parameter		Description	Example Value
Configure Listener	Name	Listener name.	HSS-outside-anp-Listener
	Protocol	Protocol used by the client and listener to distribute traffic.	TCP
	Frontend Port	Port used by the client and listener to distribute traffic.	8091
	Access Control	Supports access control based on the whitelist and blacklist.	All IP addresses
Configure Routing Policy	Backend Server Group	A group of backend servers with the same features. ● **New** ● **Use existing**	New
	Backend Server Group Name	Name of the backend server group.	HSS-outside-anp-server-group
	Backend Protocol	Specifies the protocol that backend servers in the backend server group use to receive requests from the listeners. The protocol varies depending on the forwarding mode.	TCP

Parameter		Description	Example Value
	Load Balancing Algorithm	Algorithm used by the load balancer. ● **Weighted round robin**: Requests are routed to different servers based on their weights. Backend servers with higher weights receive proportionately more requests, whereas equal-weighted servers receive the same number of requests. ● **Weighted least connections**: In addition to the number of connections, each server is assigned a weight based on its capacity. Requests are routed to the server with the lowest connections-to-weight ratio. ● **Source IP hash**: Allows requests from different clients to be routed based on source IP addresses and ensures that requests from the same client are forwarded to the same server.	Weighted round robin
Add Backend Server	Backend Servers	When you use ELB to route requests, ensure that at least one backend server is running properly and can receive requests routed by the load balancer. Click **Add Backend Server**.	HSS-outside-anp-ECS Set the service port to 8091. (Server created in **Step 3: Create an ECS**)

Step 7 On the **Confirm** page, check parameter settings.

Step 8 Click **Submit** complete the configuration.

----End

Step 6: Modify a Security Group

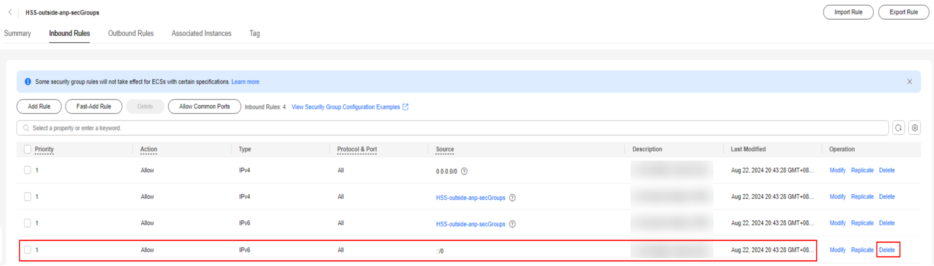
Step 1 Click ☰ in the upper left corner of the management console and choose **Network** > **Virtual Private Cloud**.

Step 2 In the navigation tree on the left, choose **Security Groups**.

Step 3 Locate the security group created in **Step 2: Create a Security Group** and click **Manage Rules**.

Step 4 Delete the IPv6 full passing rule, as shown in **Figure 11-6**.

Figure 11-6 Deleting the IPv6 full passing rule



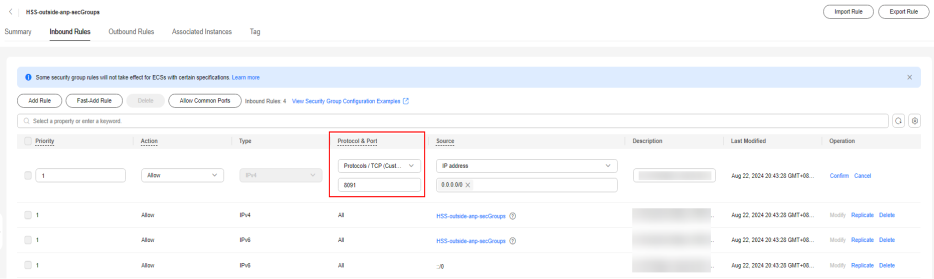
Some security group rules will not take effect for ECSs with certain specifications. Learn more

Priority	Action	Type	Protocol & Port	Source	Description	Last Modified	Operation
1	Allow	IPv4	All	0.0.0.0/0	[redacted]	Aug 22, 2024 20:43:28 GMT+08...	Modify Replicate Delete
1	Allow	IPv4	All	HSS-outside-anp-secGroups	[redacted]	Aug 22, 2024 20:43:28 GMT+08...	Modify Replicate Delete
1	Allow	IPv6	All	HSS-outside-anp-secGroups	[redacted]	Aug 22, 2024 20:43:28 GMT+08...	Modify Replicate Delete
1	Allow	IPv6	All	::/0	[redacted]	Aug 22, 2024 20:43:28 GMT+08...	Modify Replicate Delete

Step 5 Modify the IPv4 full bypass rule, as shown in **Figure 11-7**.

1. Change the value of **Protocol & Port** from **Protocols > All** to **Protocols / TCP (Custom ports)** and set the port number to **8091**.
2. Click **OK**.

Figure 11-7 Modifying the IPv4 full passing rule



Some security group rules will not take effect for ECSs with certain specifications. Learn more

Priority	Action	Type	Protocol & Port	Source	Description	Last Modified	Operation
1	Allow	IPv4	Protocols / TCP (Cust... 8091	IP address 0.0.0.0/0	[redacted]	Aug 22, 2024 20:43:28 GMT+08...	Confirm Cancel
1	Allow	IPv4	All	HSS-outside-anp-secGroups	[redacted]	Aug 22, 2024 20:43:28 GMT+08...	Modify Replicate Delete
1	Allow	IPv6	All	HSS-outside-anp-secGroups	[redacted]	Aug 22, 2024 20:43:28 GMT+08...	Modify Replicate Delete
1	Allow	IPv6	All	::/0	[redacted]	Aug 22, 2024 20:43:28 GMT+08...	Modify Replicate Delete

----End

Step 7: Prepare the kubeconfig File

The kubeconfig file specifies the cluster permissions assigned to HSS. The kubeconfig file configured using method 1 contains the cluster administrator permissions, whereas the file generated using method 2 contains only the permissions required by HSS. If you want to minimize HSS permissions, prepare the file using method 2.

- **Method 1: configuring the default kubeconfig file**
  a. Perform the following operations to create a dedicated namespace for HSS:
     i. Log in to a cluster node.
     ii. Create the **hss.yaml** file and copy the following content to the file:
     ```
     {"metadata":{"name":"hss"},"apiVersion":"v1","kind":"Namespace"}
     ```
     iii. Run the following command to create a namespace:
     ```
     kubectl apply -f hss.yaml
     ```
  b. Find and download the **config** file in the **$HOME/.kube/config** directory.
  c. Change the file name from **config** to **config.yaml**.
- **Method 2: generating a kubeconfig file dedicated to HSS**
  a. Create a dedicated namespace and an account for HSS.
     i. Log in to a cluster node.

ii. Create the **hss-account.yaml** file and copy the following content to the file:

```
{"metadata":{"name":"hss"},"apiVersion":"v1","kind":"Namespace"}{"metadata":{"name":"hss-user","namespace":"hss"},"apiVersion":"v1","kind":"ServiceAccount"}{"metadata":{"name":"hss-user-token","namespace":"hss","annotations":{"kubernetes.io/service-account.name":"hss-user"}},"apiVersion":"v1","kind":"Secret","type":"kubernetes.io/service-account-token"}
```

iii. Run the following command to create a namespace and an account:

```
kubectl apply -f hss-account.yaml
```

b. Generate the kubeconfig file.

i. Create the **gen_kubeconfig.sh** file and copy the following content to the file:

```
#!/bin/bash

KUBE_APISERVER=`kubectl config view  --output=jsonpath='{.clusters[].cluster.server}' | head -n1 `
CLUSTER_NAME=`kubectl config view -o jsonpath='{.clusters[0].name}'`
kubectl get secret hss-user-token -n hss -o yaml |grep ca.crt: | awk '{print $2}' |base64 -d >hss_ca_crt

kubectl config set-cluster ${CLUSTER_NAME} --server=${KUBE_APISERVER}  --certificate-authority=hss_ca_crt  --embed-certs=true --kubeconfig=hss_kubeconfig.yaml
kubectl config set-credentials hss-user --token=$(kubectl describe secret hss-user-token -n hss | awk '/token:/{print $2}') --kubeconfig=hss_kubeconfig.yaml
kubectl config set-context hss-user@kubernetes --cluster=${CLUSTER_NAME} --user=hss-user --kubeconfig=hss_kubeconfig.yaml
kubectl config use-context hss-user@kubernetes --kubeconfig=hss_kubeconfig.yaml
```

ii. Run the following command to generate the kubeconfig file named **hss_kubeconfig.yaml**:

```
bash gen_kubeconfig.sh
```

Step 8: Install the Agent for a Third-Party Public Network Cluster

Step 1 Log in to the management console.

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

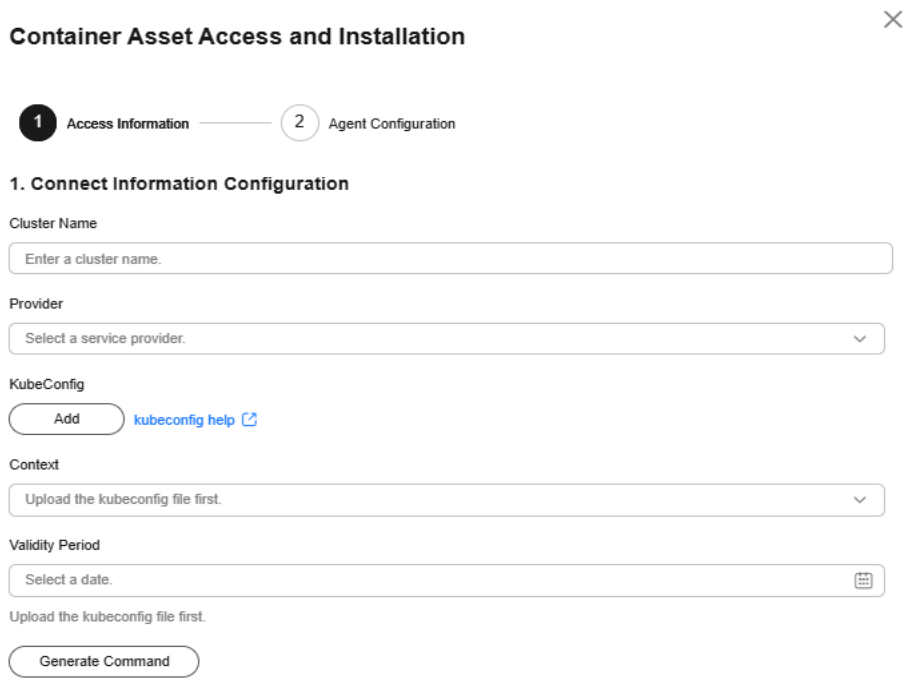
Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 On the **Cluster** tab page, click **Install Container Agent**. The **Container Asset Access and Installation** slide-out panel is displayed.

Step 5 Select **Non-CCE cluster (Internet access)** and click **Configure Now**.

Step 6 Configure cluster access information and click **Generate Command**. For more information, see **Table 11-10**.

Figure 11-8 Configuring cluster access information



Container Asset Access and Installation

1. Connect Information Configuration

Cluster Name

Enter a cluster name.

Provider

Select a service provider.

KubeConfig

Context

Upload the kubeconfig file first.

Validity Period

Select a date.

Upload the kubeconfig file first.

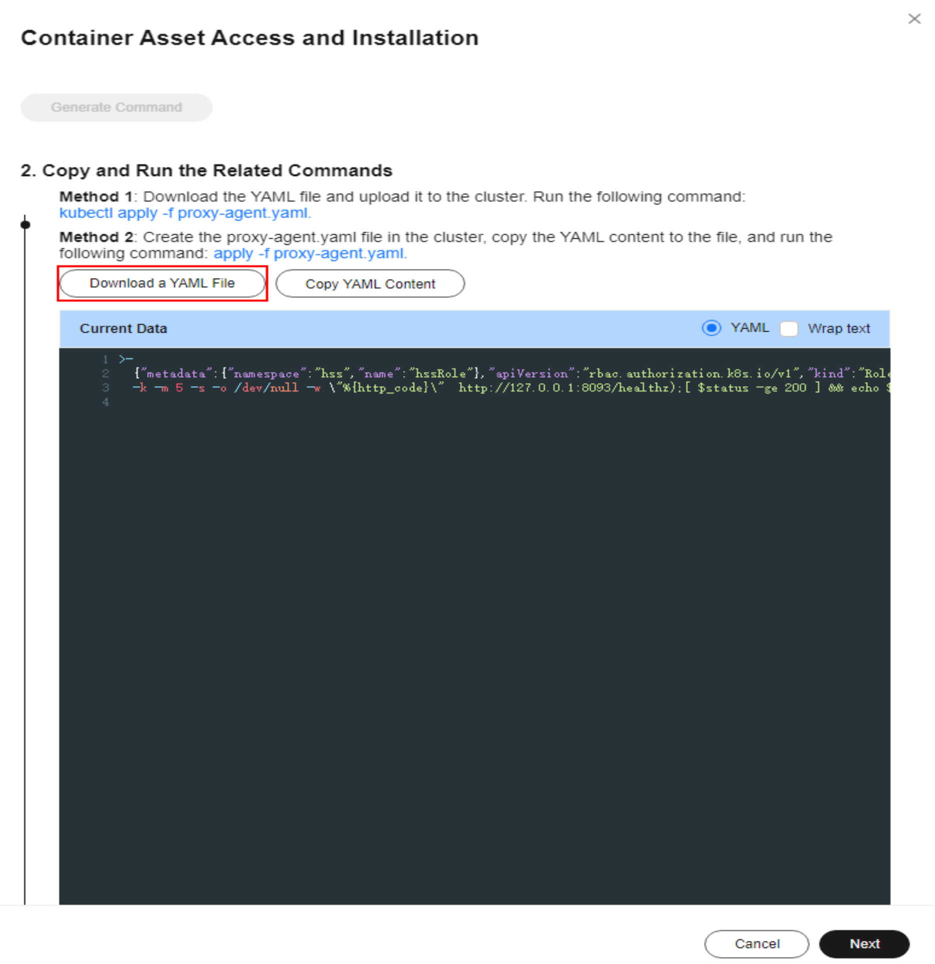
Table 11-10 Access parameters

Parameter	Description
Cluster Name	Name of the cluster to be connected.
Provider	Service provider of the cluster. Currently, the clusters of the following service providers are supported: ● Alibaba Cloud ● Tencent Cloud ● AWS ● Azure ● User-built ● On-premises IDC
KubeConfig	Add and upload the **kubeconfig.yaml** or **config.yaml** file configured as required in **Step 7: Prepare the kubeconfig File**.
Context	After the kubeconfig file is uploaded, HSS automatically parses the context.
Validity Period	After the kubeconfig file is uploaded, HSS automatically parses the validity period. You can also specify a time before the final validity period. After the specified validity period expires, you need to connect to the asset again.

Step 7 Perform the following operations to install the cluster connection component (ANP-agent) and establish a connection between HSS and the cluster:

1. In the **Container Asset Access and Installation** dialog box, click **Download a YAML File**.

Figure 11-9 Downloading the YAML file



Container Asset Access and Installation

2. Copy and Run the Related Commands

Method 1: Download the YAML file and upload it to the cluster. Run the following command: kubectl apply -f proxy-agent.yaml.

Method 2: Create the proxy-agent.yaml file in the cluster, copy the YAML content to the file, and run the following command: apply -f proxy-agent.yaml.

```
>-
  {"metadata":{"namespace":"hss","name":"hssRole"},"apiVersion":"rbac.authorization.k8s.io/v1","kind":"Rol
  -k -m 5 -s -o /dev/null -w \"%{http_code}\"  http://127.0.0.1:8093/healthz);[ $status -ge 200 ] && echo $
```

2. Copy the file to the directory of any node and run the following command to replace the proxy address:

```
sed -i 's#proxy-server-host=.*","--proxy-server-port#proxy-server-host={{Forwarding address}}","--proxy-server-port#' proxy-agent.yaml
```

   Change **{{Forwarding address}}** to the public IPv4 address recorded in **Step 4** and then run the command again.

3. Run the following command to install the cluster connection component (ANP-Agent):

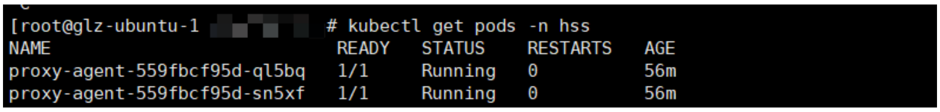
```
kubectl apply -f proxy-agent.yaml
```

4. Run the following command to check whether the cluster connection component (ANP-agent) is successfully installed:

```
kubectl get pods -n hss | grep proxy-agent
```

   If the command output shown in **Figure 11-10** is displayed, the cluster connection component (ANP-agent) is successfully installed.

Figure 11-10 ANP-Agent installed



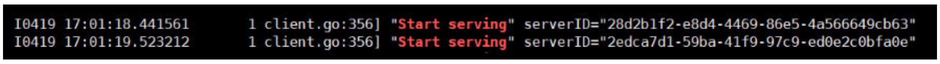
```
[root@glz-ubuntu-1 [redacted] # kubectl get pods -n hss
NAME                            READY   STATUS    RESTARTS   AGE
proxy-agent-559fbcf95d-ql5bq    1/1     Running   0          56m
proxy-agent-559fbcf95d-sn5xf    1/1     Running   0          56m
```

5. Run the following command to check whether the cluster is connected to HSS:

```
for a in $(kubectl get pods -n hss| grep proxy-agent | cut -d ' ' -f1); do kubectl -n hss logs $a | grep 'Start serving';done
```

   If the command output shown in **Figure 11-11** is displayed, the cluster is connected to HSS.

Figure 11-11 Cluster connected to HSS



```
I0419 17:01:18.441561       1 client.go:356] "Start serving" serverID="28d2b1f2-e8d4-4469-86e5-4a566649cb63"
I0419 17:01:19.523212       1 client.go:356] "Start serving" serverID="2edca7d1-59ba-41f9-97c9-ed0e2c0bfa0e"
```

Step 8 In the **Container Asset Access and Installation** dialog box, click **Next**.

Step 9 Configure agent parameters. For more information, see **Table 11-11**.

Table 11-11 Agent parameters

Parameter	Description
Configuration Rules	Select an agent configuration rule. ● **Default Rule**: Select this if the sock address of container runtime is a common address. The agent will be installed on nodes having no taints. ● **Custom**: Select this rule if the sock address of your container runtime is not a common address or needs to be modified, or if you only want to install the agent on specific nodes. NOTE ● If the sock address of your container runtime is incorrect, some HSS functions may be unavailable after the cluster is connected to HSS. ● You are advised to select all runtime types.

Parameter	Description
(Optional) Advanced Configuration	This parameter can be set if **Custom** is selected for **Configuration Rules**. Click ⌄ to expand advanced configurations. The **Enabling auto upgrade agent** option is selected by default. ● **Enabling auto upgrade** Configure whether to enable automatic agent upgrade. If it is enabled, HSS automatically upgrades the agent to the latest version between 00:00 to 06:00 every day to provide you with better services. ● **Node Selector Configuration** Set the **Key** and **Value** of tags of the nodes where the agent is to be installed and click **Add**. If no tags are specified, the agent will be installed on all the nodes having no taints. ● **Tolerance Configuration** If you added a node whose tag contains a taint in **Node Selector Configuration**, set the **Key**, **Value**, and **Effect** of the taint, and click **Add** to allow agent installation on the node.

Step 10 Click **OK** to start installing the HSS agent.

Step 11 In the cluster list, check the cluster status. If the cluster status is **Running**, the cluster is successfully connected to HSS.

----End

Follow-up Procedure

After the agent is installed in a cluster, **enable protection**.

FAQ

- **What Do I Do If the Cluster Connection Component (ANP-Agent) Failed to Be Deployed?**
- **What Do I Do If Cluster Permissions Are Abnormal?**

11.1.5 Installing the Agent in a Third-Party Private Network Cluster

Scenario

Install the agent on a third-party private network cluster that cannot access the public network. After the configuration is complete, HSS automatically installs the agent on existing cluster nodes, installs the agent on new nodes when the cluster is scaled out, and uninstalls the agent from removed nodes when the cluster is scaled in.

Prerequisites

A Direct Connect connection has been created between the third-party private network cluster and the VPC on the cloud. For details about how to create a Direct Connect connection, see **Getting Started with Direct Connect**.

Constraints

- Supported cluster orchestration platforms: Kubernetes 1.19 or later
- Supported node OS: Linux
- Node specifications: at least 2 vCPUs, 4 GiB memory, 40 GiB system disk, and 100 GiB data disk
- Constraints on private clusters to access regions: Currently, only CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, AP-Hong Kong, AP-Singapore, CN Southwest-Guiyang1, and AP-Jakarta allow third-party cloud clusters or on-premises clusters to access HSS through private networks.
- The agent is incompatible with clusters of Galera 3.34, MySQL 5.6.51, or earlier versions.

Step 1: Create an ECS

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

Step 2 Configure ECS parameters as prompted.

You are advised to configure some parameters by referring to **Table 11-12** and configure other parameters based on site requirements.

Table 11-12 Parameters for purchasing an ECS

Parameter	Description	Example Value
Billing Mode	ECS billing mode. ● Yearly/Monthly: Prepaid mode. Yearly/monthly ECSs are billed by the purchased duration specified in the order. ● Pay-per-use: Postpaid billing mode. You pay as you go and just pay for what you use. Pay-per-use ECSs are billed by the second and settled by the hour. ● Spot price: Spot pricing is a postpaid billing mode. You pay as you go and just pay for what you use. In **Spot pricing** billing mode, your purchased ECS is billed at a lower price than that of a pay-per-use ECS with the same specifications. In **Spot pricing** billing mode, you can select **Spot** or **Spot block** for the **Spot Type**. Spot ECSs and Spot block ECSs are billed by the second and settled by the hour.	Pay-per-use

Parameter	Description	Example Value
CPU Architecture	Select a CPU architecture. The value can be **x86** or **Kunpeng**.	x86
Instance	● Select vCPUs and memory, or enter a keyword to search for ECS specifications. You can search for ECS flavors when you select **By Type**. ● Select ECS specifications by instance family and generation from the list.	General computing, 2 vCPUs, 4 GiB
Image	An image is an ECS template that contains an OS. It may also contain proprietary software and application software. You can use images to create ECSs.	Public image, EulerOS 2.5 64 bit (40 GiB)
System Disk	Stores the OS of an ECS, and is automatically created and initialized upon ECS creation.	Ultra-high I/O

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

Step 4 In the ECS list, view the created ECS and record its private IP address.

----End

Step 2: Set Up Nginx

Step 1 Log in to the server created in **Step 1: Create an ECS**.

Step 2 Go to the **temp** directory.

cd /temp

Step 3 Run the following command to create the **install_nginx.sh** file:

vi install_nginx.sh

Step 4 Press **i** to enter the editing mode and copy the following content to the **install_nginx.sh** file:

```
#!/bin/bash

yum -y install pcre-devel zlib-devel popt-devel openssl-devel openssl
wget http://www.nginx.org/download/nginx-1.21.0.tar.gz
tar zxf nginx-1.21.0.tar.gz -C /usr/src/
cd /usr/src/nginx-1.21.0/
useradd -M -s /sbin/nologin nginx
./configure \
--prefix=/usr/local/nginx \
--user=nginx \
--group=nginx \
--with-file-aio \
--with-http_stub_status_module \
--with-http_gzip_static_module \
--with-http_flv_module \
--with-http_ssl_module \
--with-stream \
--with-pcre && make && make install
ln -s /usr/local/nginx/sbin/nginx /usr/local/sbin/
nginx
```

Step 5 Enter **ECS**, run the following command, and press **Enter** to exit.

:wq!

Step 6 Run the following command to install Nginx:

bash /temp/install_nginx.sh

Step 7 Run the following command to modify the Nginx configuration file:

```
cat <<END >> /usr/local/nginx/conf/nginx.conf
stream {
  upstream backend_hss_anp {
    server {{ANP_backend_address}}:8091 weight=5 max_fails=3 fail_timeout=30s;
  }
  server {
    listen 8091 so_keepalive=on;
    proxy_connect_timeout 10s;
    proxy_timeout 300s;
    proxy_pass backend_hss_anp ;
  }
}
END
```

Replace **{{ANP_backend_address}}** with the actual address and then run the command. For details, see **Table 11-13**.

Table 11-13 ANP backend addresses

Region	ANP Backend Address
Guiyang1, Bangkok, Shanghai2, Guangzhou, Beijing4, Beijing2, and Shanghai1	hss-proxy.RegionCode.myhuaweicloud.com
Other	hss-anp.RegionCode.myhuaweicloud.com
For details about region codes, see **Regions and Endpoints**.	

Step 8 Run the following command to make the Nginx configuration take effect:

nginx -s reload

----End

Step 3: Prepare the kubeconfig File

The kubeconfig file specifies the cluster permissions assigned to HSS. The kubeconfig file configured using method 1 contains the cluster administrator permissions, whereas the file generated using method 2 contains only the permissions required by HSS. If you want to minimize HSS permissions, prepare the file using method 2.

- **Method 1: configuring the default kubeconfig file**

a. Perform the following operations to create a dedicated namespace for HSS:

   i. Log in to a cluster node.

   ii. Create the **hss.yaml** file and copy the following content to the file:
```
{"metadata":{"name":"hss"},"apiVersion":"v1","kind":"Namespace"}
```

   iii. Run the following command to create a namespace:
```
kubectl apply -f hss.yaml
```

b. Find and download the **config** file in the **$HOME/.kube/config** directory.

c. Change the file name from **config** to **config.yaml**.

- **Method 2: generating a kubeconfig file dedicated to HSS**

a. Create a dedicated namespace and an account for HSS.

   i. Log in to a cluster node.

   ii. Create the **hss-account.yaml** file and copy the following content to the file:
```
{"metadata":{"name":"hss"},"apiVersion":"v1","kind":"Namespace"}{"metadata":
{"name":"hss-user","namespace":"hss"},"apiVersion":"v1","kind":"ServiceAccount"}
{"metadata":{"name":"hss-user-token","namespace":"hss","annotations":{"kubernetes.io/
service-account.name":"hss-user"}},"apiVersion":"v1","kind":"Secret","type":"kubernetes.io/
service-account-token"}
```

   iii. Run the following command to create a namespace and an account:
```
kubectl apply -f hss-account.yaml
```

b. Generate the kubeconfig file.

   i. Create the **gen_kubeconfig.sh** file and copy the following content to the file:
```
#!/bin/bash

KUBE_APISERVER=`kubectl config view  --output=jsonpath='{.clusters[].cluster.server}' |
head -n1 `
CLUSTER_NAME=`kubectl config view -o jsonpath='{.clusters[0].name}'`
kubectl get secret hss-user-token -n hss -o yaml |grep ca.crt: | awk '{print $2}' |base64 -d
>hss_ca_crt

kubectl config set-cluster ${CLUSTER_NAME} --server=${KUBE_APISERVER}  --certificate-
authority=hss_ca_crt  --embed-certs=true --kubeconfig=hss_kubeconfig.yaml
kubectl config set-credentials hss-user --token=$(kubectl describe secret hss-user-token -n
hss | awk '/token:/{print $2}') --kubeconfig=hss_kubeconfig.yaml
kubectl config set-context hss-user@kubernetes --cluster=${CLUSTER_NAME} --user=hss-
user --kubeconfig=hss_kubeconfig.yaml
kubectl config use-context hss-user@kubernetes --kubeconfig=hss_kubeconfig.yaml
```

   ii. Run the following command to generate the kubeconfig file named **hss_kubeconfig.yaml**:
```
bash gen_kubeconfig.sh
```

Step 4: Install the Agent for a Third-Party Private Network Cluster

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 On the **Cluster** tab page, click **Install Container Agent**. The **Container Asset Access and Installation** slide-out panel is displayed.

Step 5 Select **Non-CCE cluster (private network access)** and click **Configure Now**.

Step 6 Configure image repository information and click **Generate Command**. For more information, see **Table 11-14**.

Table 11-14 Image repository parameters

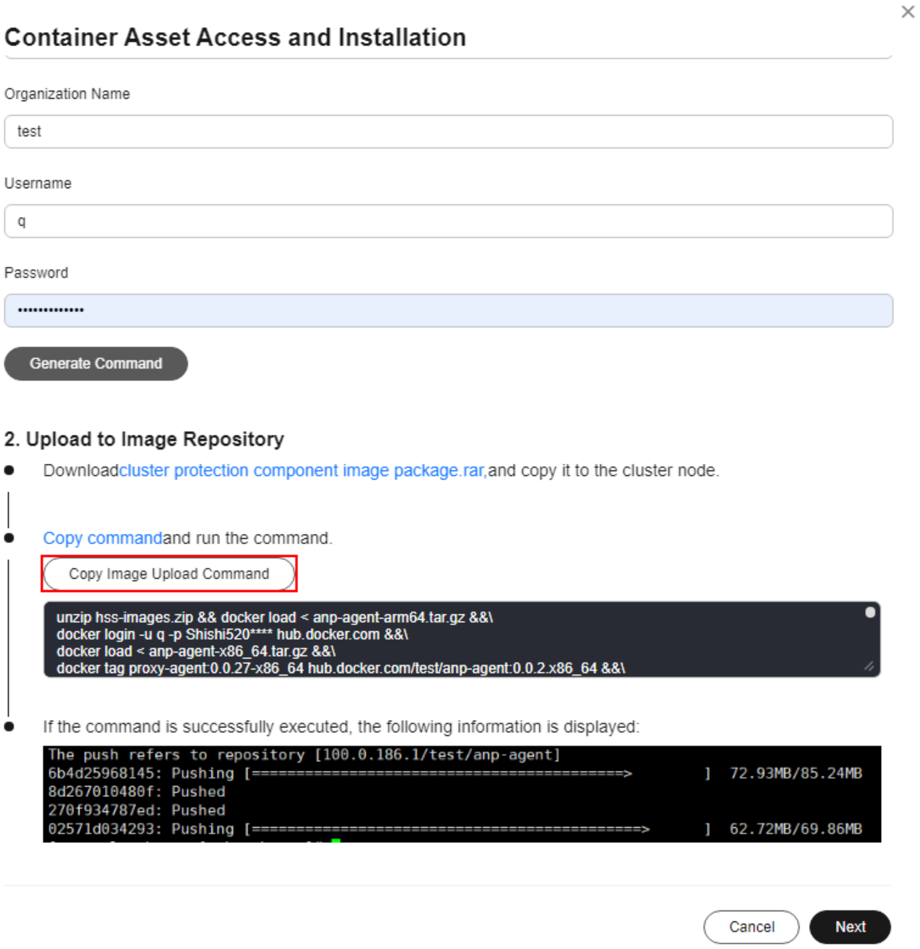
Parameter	Description
Third-Party Image Repository Address	Third-party image repository address. Example: **hub.docker.com**
Image Repository Type	Type of the image repository. It can be: ● **Harbor** ● **Quay** ● **Jfrog** ● **Other**
Organization Name	Organization name of the image repository.
Username	Image repository username.
Password	Password of the image repository.

Parameter	Description
Advanced Configuration	- **Image Architecture** Optional. You can select the image architecture used by a container. By default, the container uses a multi-architecture image. - **ANP Proxy Address** Enter the private IP address of the server created in **Step 1: Create an ECS**. - **Hostguard Proxy Address** Private IP address of a Direct Connect server (port 10180). - **Container Name** After a cluster is connected to HSS, ANP-agent and Hostguard (the HSS agent) will run on nodes as containers. To identify these containers, set easily distinguishable names for them. - **DNS Configuration** The DNS of the pod is configured in Kubernetes, so that you can search for a service in a running container by its name instead of IP address. You can configure DNS for the pods of the ANP-agent and Hostguard (the HSS agent) to facilitate search. Options are as follows: – **Default**: The pod inherits the domain name resolution configuration from the node where the pod is running. – **ClusterFirst**: Any DNS query (for example, **www.kubernetes.io**) that does not match the configured cluster domain suffix is forwarded by the DNS server to the upstream DNS server. Cluster administrators may have extra stub-domain and upstream DNS servers configured. – **ClusterFirstWithHostNet**: For the pods running in hostNetwork mode, the DNS policy should be explicitly set to **ClusterFirstWithHostNet**. Otherwise, the pods that run in hostNetwork mode and use the **ClusterFirst** policy will roll back to the **Default** policy. – **None**: If the pod's **dnsPolicy** is set to **None**, the list must contain at least one IP address, otherwise this property is optional. The listed servers will be combined with the base domain name servers generated using a specified DNS policy, and duplicate addresses will be removed.

Step 7 Perform the following operations to upload the images of the cluster connection component (ANP-agent) and the HSS agent to your private image repository:

1. In the **Access and Install Container Assets** dialog box, click **cluster protection component image package.rar** to download the package to the local PC and copy the package to any cluster node.
2. In the **Container Asset Access and Installation** dialog box, click **Copy Image Upload Command** to copy the command and run it on the cluster node.

Figure 11-12 Copying image upload commands



Container Asset Access and Installation

Organization Name
test

Username
q

Password
•••••••••••••

2. Upload to Image Repository

- Downloadcluster protection component image package.rar,and copy it to the cluster node.
- Copy commandand run the command.

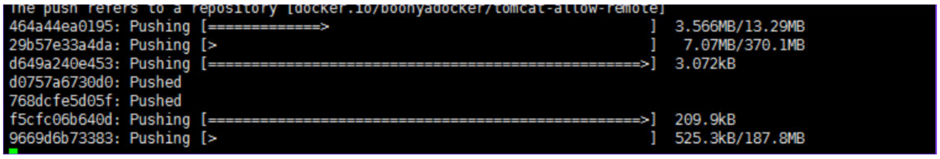
```
unzip hss-images.zip && docker load < anp-agent-arm64.tar.gz &&\
docker login -u q -p Shishi520**** hub.docker.com &&\
docker load < anp-agent-x86_64.tar.gz &&\
docker tag proxy-agent:0.0.27-x86_64 hub.docker.com/test/anp-agent:0.0.2.x86_64 &&\
```

- If the command is successfully executed, the following information is displayed:

```
The push refers to repository [100.0.186.1/test/anp-agent]
6b4d25968145: Pushing [=========================================>         ]  72.93MB/85.24MB
8d267010480f: Pushed
270f934787ed: Pushed
02571d034293: Pushing [===========================================>       ]  62.72MB/69.86MB
```

If the command output shown in **Figure 11-13** is displayed, the upload succeeded.

Figure 11-13 Image uploaded

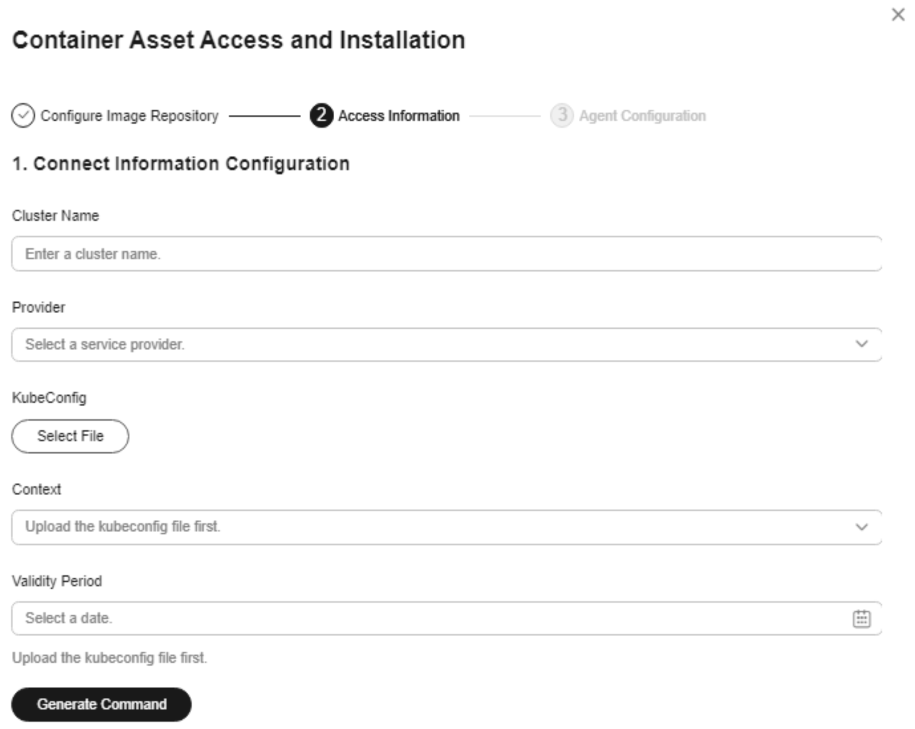


```
The push refers to a repository [docker.io/boonyadocker/tomcat-allow-remote]
464a44ea0195: Pushing [=============>                                     ]  3.566MB/13.29MB
29b57e33a4da: Pushing [>                                                  ]   7.07MB/370.1MB
d649a240e453: Pushing [==================================================>]  3.072kB
d0757a6730d0: Pushed
768dcfe5d05f: Pushed
f5cfc06b640d: Pushing [==================================================>]  209.9kB
9669d6b73383: Pushing [>                                                  ]  525.3kB/187.8MB
```

Step 8 In the **Container Asset Access and Installation** dialog box, click **Next**.

Step 9 Configure cluster access information and click **Generate Command**. For more information, see **Table 11-15**.

Figure 11-14 Configuring cluster access information



Container Asset Access and Installation

1. Connect Information Configuration

Cluster Name: Enter a cluster name.

Provider: Select a service provider.

KubeConfig: Select File

Context: Upload the kubeconfig file first.

Validity Period: Select a date.

Upload the kubeconfig file first.

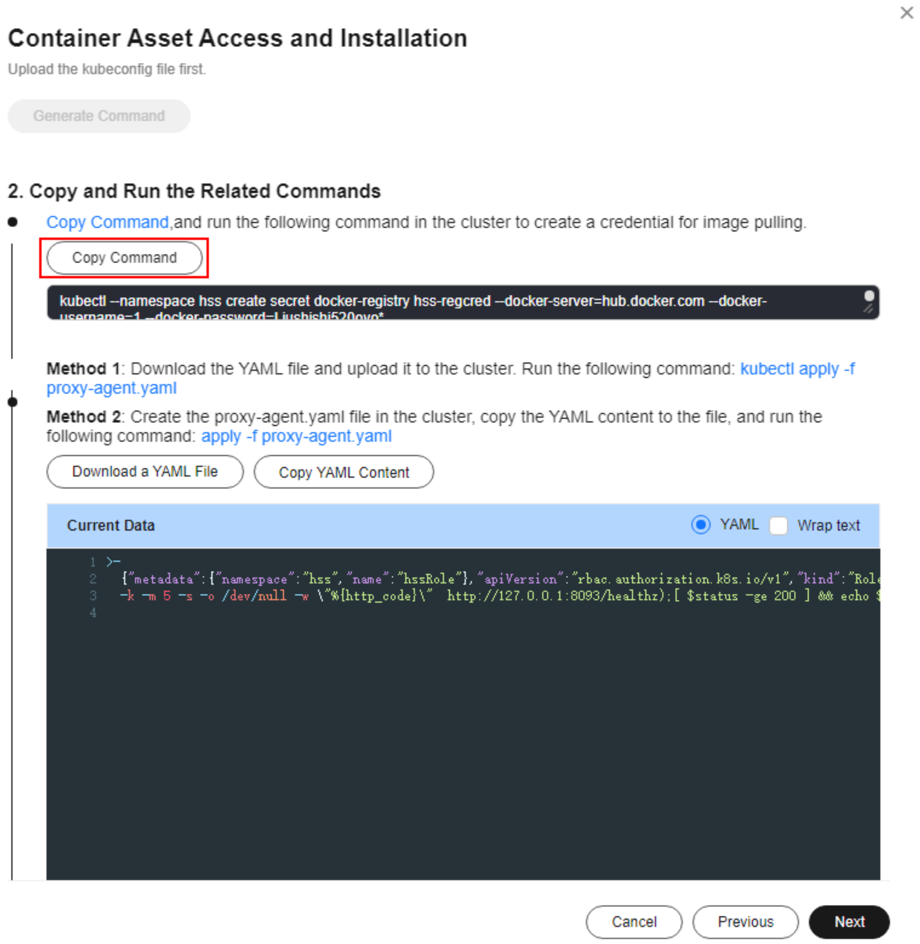
Table 11-15 Access parameters

Parameter	Description
Cluster Name	Name of the cluster to be connected.
Provider	Service provider of the cluster. Currently, the clusters of the following service providers are supported: ● Alibaba Cloud ● Tencent Cloud ● AWS ● Azure ● User-built ● On-premises IDC
KubeConfig	Add and upload the kubeconfig file configured as required in **Step 3: Prepare the kubeconfig File**.
Context	After the kubeconfig file is uploaded, HSS automatically parses the context.
Validity Period	After the kubeconfig file is uploaded, HSS automatically parses the validity period. You can also specify a time before the final validity period. After the specified validity period expires, you need to connect to the asset again.

Step 10 Perform the following operations to install the cluster connection component (ANP-agent) and establish a connection between HSS and the cluster:

1. In the **Container Asset Access and Installation** dialog box, click **Copy Command**.

Figure 11-15 Copying the command



Container Asset Access and Installation

Upload the kubeconfig file first.

Generate Command

2. Copy and Run the Related Commands

- Copy Command,and run the following command in the cluster to create a credential for image pulling.

Copy Command

```
kubectl --namespace hss create secret docker-registry hss-regcred --docker-server=hub.docker.com --docker-
username=1 --docker-password=Liushishi520ovo*
```

Method 1: Download the YAML file and upload it to the cluster. Run the following command: kubectl apply -f proxy-agent.yaml

Method 2: Create the proxy-agent.yaml file in the cluster, copy the YAML content to the file, and run the following command: apply -f proxy-agent.yaml

Download a YAML File   Copy YAML Content

Current Data   ● YAML □ Wrap text

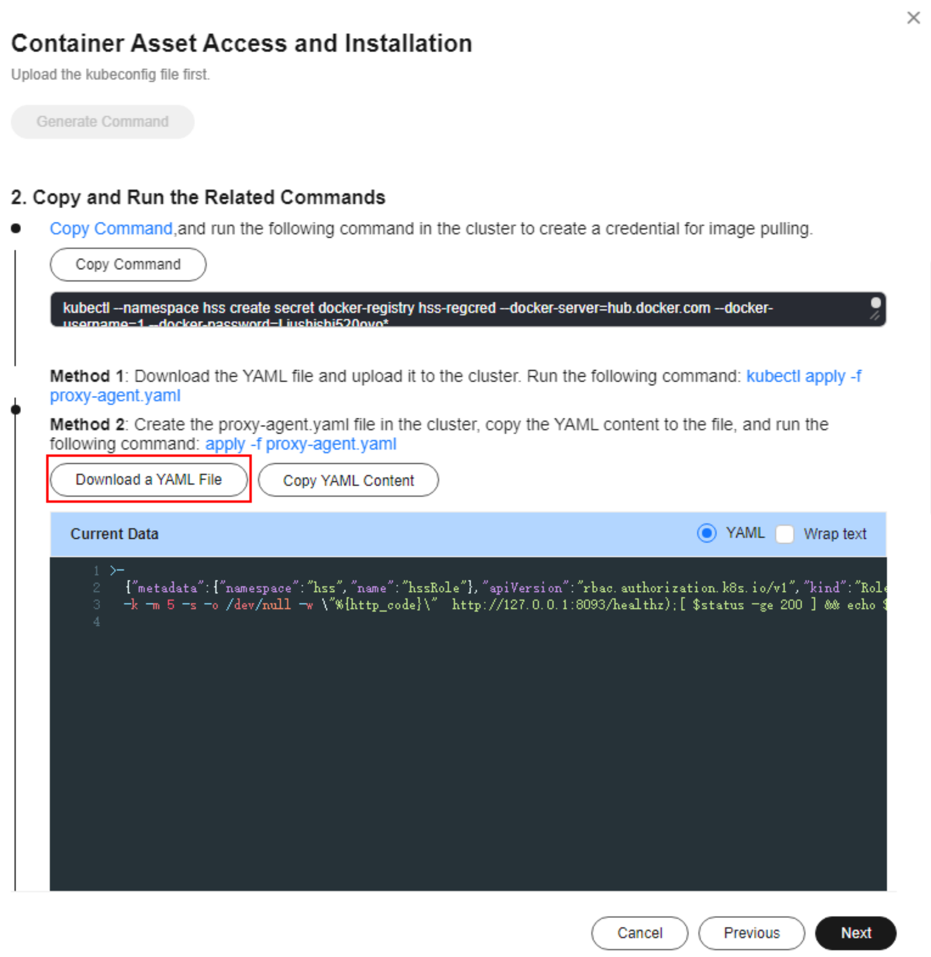
```
>-
  {"metadata":{"namespace":"hss","name":"hssRole"},"apiVersion":"rbac.authorization.k8s.io/v1","kind":"Role
  -k -m 5 -s -o /dev/null -w \"%{http_code}\"  http://127.0.0.1:8093/healthz);[ $status -ge 200 ] && echo $

```

2. Log in to a node and run the copied command to create a credential for the cluster to pull private images:

3. In the **Container Asset Access and Installation** dialog box, click **Download a YAML File**.

Figure 11-16 Downloading the YAML file



Container Asset Access and Installation

Upload the kubeconfig file first.

2. Copy and Run the Related Commands

- Copy Command,and run the following command in the cluster to create a credential for image pulling.

```
kubectl --namespace hss create secret docker-registry hss-regcred --docker-server=hub.docker.com --docker-
username=1 --docker-password=Liushishi520ovo*
```

Method 1: Download the YAML file and upload it to the cluster. Run the following command: kubectl apply -f proxy-agent.yaml

Method 2: Create the proxy-agent.yaml file in the cluster, copy the YAML content to the file, and run the following command: apply -f proxy-agent.yaml

```
>-
  {"metadata":{"namespace":"hss","name":"hssRole"},"apiVersion":"rbac.authorization.k8s.io/v1","kind":"Role
  -k -m 5 -s -o /dev/null -w \"%{http_code}\"  http://127.0.0.1:8093/healthz);[ $status -ge 200 ] && echo $
```

4. Copy the file to the directory of any node.
5. Run the following command to install the cluster connection component (ANP-Agent):

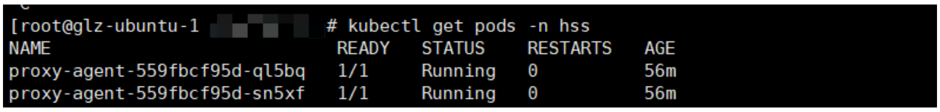
```
kubectl apply -f proxy-agent.yaml
```

6. Run the following command to check whether the cluster connection component (ANP-agent) has been installed:

```
kubectl get pods -n hss | grep proxy-agent
```

If the command output shown in **Figure 11-17** is displayed, the cluster connection component (ANP-agent) is successfully installed.

Figure 11-17 ANP-Agent installed



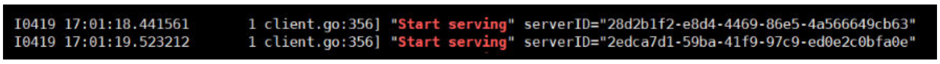
```
[root@glz-ubuntu-1 [redacted]  # kubectl get pods -n hss
NAME                          READY   STATUS    RESTARTS   AGE
proxy-agent-559fbcf95d-ql5bq  1/1     Running   0          56m
proxy-agent-559fbcf95d-sn5xf  1/1     Running   0          56m
```

7. Run the following command to check whether the cluster is connected to HSS:

```
for a in $(kubectl get pods -n hss| grep proxy-agent | cut -d ' ' -f1); do kubectl -n hss logs $a | grep
'Start serving';done
```

If the command output shown in **Figure 11-18** is displayed, the cluster is connected to HSS.

Figure 11-18 Cluster connected to HSS



```
I0419 17:01:18.441561       1 client.go:356] "Start serving" serverID="28d2b1f2-e8d4-4469-86e5-4a566649cb63"
I0419 17:01:19.523212       1 client.go:356] "Start serving" serverID="2edca7d1-59ba-41f9-97c9-ed0e2c0bfa0e"
```

Step 11 In the **Container Asset Access and Installation** dialog box, click **Next**.

Step 12 Configure agent parameters. For more information, see **Table 11-16**.

Table 11-16 Agent parameters

Parameter	Description
Configuration Rules	Select an agent configuration rule. ● **Default Rule**: Select this if the sock address of container runtime is a common address. The agent will be installed on nodes having no taints. ● **Custom**: Select this rule if the sock address of your container runtime is not a common address or needs to be modified, or if you only want to install the agent on specific nodes. **NOTE** ● If the sock address of your container runtime is incorrect, some HSS functions may be unavailable after the cluster is connected to HSS. ● You are advised to select all runtime types.
(Optional) Advanced Configuration	This parameter can be set if **Custom** is selected for **Configuration Rules**. Click ⌄ to expand advanced configurations. The **Enabling auto upgrade agent** option is selected by default. ● **Enabling auto upgrade** Configure whether to enable automatic agent upgrade. If it is enabled, HSS automatically upgrades the agent to the latest version between 00:00 to 06:00 every day to provide you with better services. ● **Node Selector Configuration** Set the **Key** and **Value** of tags of the nodes where the agent is to be installed and click **Add**. If no tags are specified, the agent will be installed on all the nodes having no taints. ● **Tolerance Configuration** If you added a node whose tag contains a taint in **Node Selector Configuration**, set the **Key**, **Value**, and **Effect** of the taint, and click **Add** to allow agent installation on the node.

Step 13 Click **OK** to start installing the HSS agent.

Step 14 In the cluster list, check the cluster status. If the cluster status is **Running**, the cluster is successfully connected to HSS.

----End

Follow-up Procedure

After the agent is installed in a cluster, **enable protection**.

FAQ

- **What Do I Do If the Cluster Connection Component (ANP-Agent) Failed to Be Deployed?**
- **What Do I Do If Cluster Permissions Are Abnormal?**
- **Failed to Upload the Image to the Private Image Repository**

11.2 Installing the Agent on an Independent Container Node

The method of installing the agent on an independent node is the same as that of installing the agent on a common server. You simply need to install the agent on the node. For details, see **Installing the Agent on Servers**.

11.3 Modifying Cluster Agent Installation Information

Scenario

You can modify the access information in the following cases:

- In a non-CCE cluster accessed through a private network, the image repository information has been configured and the command has been generated, but the command has not been executed on cluster nodes. In this case, you can refer to this section to go to the access information modification page and perform subsequent operations.
- In a non-CCE cluster accessed through Internet, the access information has been configured and the command has been generated, but the command has not been executed on cluster nodes. In this case, you can refer to this section to go to the access information modification page and perform subsequent operations.
- In a non-CCE cluster accessed through Internet, the specified certificate expiration date is earlier than the final expiration date, but needs to be changed to that date.
- You need to modify the scope of cluster nodes where the agent is to be installed. After the modification, the agent on all cluster nodes will be automatically uninstalled, and then the agent will be reinstalled on specified nodes.
- The container runtime type and sock address need to be modified. After the modification, the agent on all cluster nodes will be automatically uninstalled, and then the agent will be reinstalled on specified nodes.
- Automatic agent upgrade needs to be enabled or disabled.

Modifying Access Information

Step 1 Log in to the management console.

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

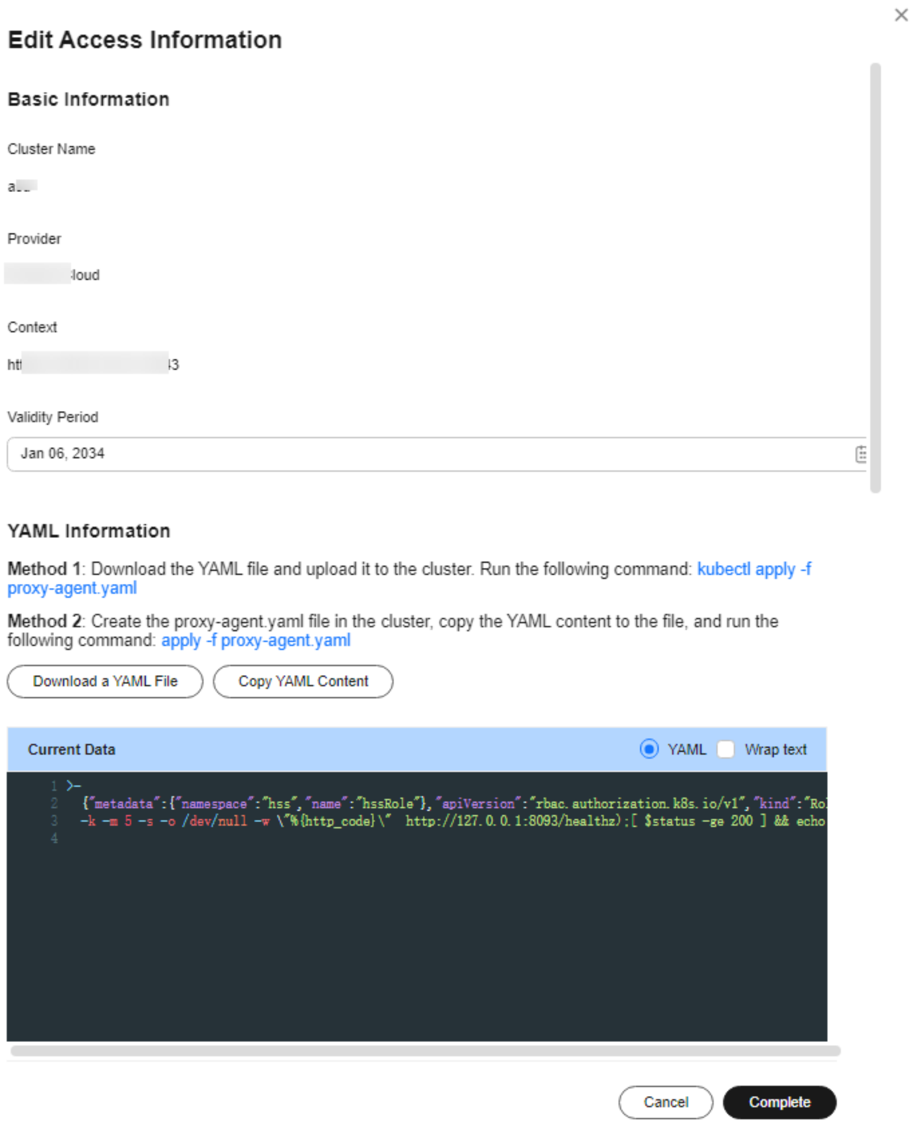
Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **Cluster** tab.

Step 5 In the row of a cluster, click **Edit Access Information** in the **Operation** column. The **Edit Access Information** dialog box is displayed.

The following figure uses the access information of a non-CCE cluster (accessed through Internet) as an example.

Figure 11-19 Edit access information



Edit Access Information

Basic Information

Cluster Name

a[redacted]

Provider

[redacted]loud

Context

ht[redacted]3

Validity Period

Jan 06, 2034

YAML Information

Method 1: Download the YAML file and upload it to the cluster. Run the following command: kubectl apply -f proxy-agent.yaml

Method 2: Create the proxy-agent.yaml file in the cluster, copy the YAML content to the file, and run the following command: apply -f proxy-agent.yaml

```
>-
  {"metadata":{"namespace":"hss","name":"hssRole"},"apiVersion":"rbac.authorization.k8s.io/v1","kind":"Ro
  -k -m 5 -s -o /dev/null -w \"%{http_code}\"  http://127.0.0.1:8093/healthz);[ $status -ge 200 ] && echo
```

Step 6 Modify access information. For details about the parameters that can be modified, see **Table 11-17**.

Table 11-17 Modifiable access parameters

Access Mode	Parameter	Description
Non-CCE cluster (Internet access)	Validity Period	You can specify a time before the final validity period. After the specified validity period expires, you need to connect to the asset again.
All access modes	Configuration Rules	Select an agent configuration rule. ● **Default Rule**: Select this if the sock address of container runtime is a common address. The agent will be installed on nodes having no taints. ● **Custom**: Select this rule if the sock address of your container runtime is not a common address or needs to be modified, or if you only want to install the agent on specific nodes. **NOTE** ● If the sock address of your container runtime is incorrect, some HSS functions may be unavailable after the cluster is connected to HSS. ● You are advised to select all runtime types.
	(Optional) Advanced Configuration	This parameter can be set if **Custom** is selected for **Configuration Rules**. Click ⌄ to expand all advanced configuration items. ● **Enabling auto upgrade agent** Configure whether to enable automatic agent upgrade. If it is enabled, HSS automatically upgrades the agent to the latest version between 00:00 to 06:00 every day to provide you with better services. ● Node Selector Configuration Select the tag of the nodes where the agent is to be installed. If this parameter is not specified, the agent will be installed on all nodes having no taints by default. ● Tolerance Configuration If the taint tag is selected in **Node Selector Configuration** and the agent needs to be installed on the taint node, you can configure taint toleration.

Step 7 Click **Complete**.

If the container runtime type, container runtime sock address, node selection configuration, or tolerance configuration is modified, the agent on all cluster nodes will be automatically uninstalled and then reinstalled. Wait until the agent installation is complete.

----End

11.4 Managing Cluster Agents

You can upgrade the agent or uninstall it from a cluster.

Prerequisites

The cluster is running.

Constraints

The agent can be upgraded only on CCE clusters. To use the latest HSS version for other types of clusters, uninstall the agent and connect it to the clusters again. For details, see **Uninstalling the Agent from a Cluster** and **Installing an Agent in a Cluster**.

Upgrading the Cluster Agent

HSS is periodically updated to improve its capabilities. You are advised to upgrade the agent to the latest version in a timely manner.

If the agent has not been upgraded for more than six months, HSS will automatically upgrade it to the latest version. In the latest version, the known issues in earlier versions are fixed, and the threat detection and defense capabilities are enhanced to improve overall security. The upgrade is performed by HSS in the time window from 22:00 to 06:00 the next day. It does not affect your services.

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

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **Cluster** tab.

Step 5 In the **Operation** column of a cluster, click **Upgrade Agent**.

To upgrade the agent on CCE clusters in batches, select all target CCE clusters and click **Upgrade Agent**.

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

Wait for 5 to 10 minutes. If the agent version in the cluster list is the latest and the **Upgrade Agent** button is grayed out, the upgrade is successful.

----End

Uninstalling the Agent from a Cluster

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **Cluster** tab.

Step 5 In the **Operation** column of a cluster, click **Uninstall Cluster**.

To uninstall CCE clusters in batches, select all target clusters and click **Uninstall Agent**. Clusters of other types cannot be uninstalled in batches.

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

Wait for 5 to 10 minutes. If the cluster is not displayed in the cluster list, the agent has been uninstalled.

----End

11.5 Viewing the Cluster Node List and Permission List

You can view the cluster node list and permission list.

Viewing the Cluster Node and Permission Lists

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **Cluster** tab.

Step 5 Click **Synchronize Access Status** to refresh the cluster access status.

Step 6 Click **Synchronize the Latest Assets**.

Step 7 Check the cluster access status.

To export the cluster list, click **Export** above the list.

Step 8 Click the name of a cluster to go to the cluster node details page and view the node and permission lists.

- Node list

  The node list displays the information about all nodes and the agent status and version.

- Permission list

The permission list displays the container-related functions and features provided by HSS, and whether the cluster has the permission to use the functions. CCE clusters have no permission lists.

----End

11.6 Managing Agents on Independent Nodes

You can upgrade the agent or uninstall it from an independent node.

Prerequisites

The agent of a node is online.

Upgrading the Agent on an Independent Node

HSS is periodically updated to improve its capabilities. You are advised to upgrade the agent to the latest version in a timely manner.

If the agent has not been upgraded for more than six months, HSS will automatically upgrade it to the latest version. In the latest version, the known issues in earlier versions are fixed, and the threat detection and defense capabilities are enhanced to improve overall security. The upgrade is performed by HSS in the time window from 22:00 to 06:00 the next day. It does not affect your services.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **Non-cluster Node** tab.

Step 5 Upgrade the agent using either of the following methods:

- Automatic upgrade

  In the upper right corner of the node list, click ○ to enable automatic upgrade. After this function is enabled, HSS automatically upgrades all agents to the latest version between 00:00 and 06:00 every day. You can view the agent version of a node after 06:00 the next day to check whether the upgrade is successful.

- Manual upgrade

  a. In the **Operation** column of a cluster, click **Upgrade Agent**.

     To upgrade the agent on CCE clusters in batches, select all target nodes and click **Upgrade Agent**.

  b. Confirm the upgrade information and click **OK**.

     Wait for 5 to 10 minutes. If the agent version of the target node is the latest, the upgrade is successful.

----End

Uninstalling the Agent from an Independent Node

Uninstall the HSS agent if you no longer need it. This section describes how to uninstall an online agent. If the agent status is offline, perform the operations in **Manually Uninstalling the Agent from a Server**.

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

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **Non-cluster Node** tab.

Step 5 In the **Operation** column of a node, click **Uninstall Agent**.

To uninstall the agent from nodes in batches, select all target nodes and click **Uninstall Agent**.

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

Wait for 5 to 10 minutes. If the agent status of the target node is **Not installed**, the uninstallation is successful.

----End

11.7 Connecting to a Third-party Image Repository

HSS can connect to third-party image repositories and provides security detection and management capabilities for vulnerabilities, baselines, and malicious files, helping you detect security risks in images in a timely manner. This section describes how to connect a third-party image repository to HSS.

Prerequisite

The repository cluster (cluster where the repository is deployed) has been connected to HSS and is in the **Running** state. For more details, see **Overview of Agent Installation in a Cluster**.

Constraints

Restrictions on the types of third-party image repositories that can be connected to HSS are as follows:

- Third-party cloud container clusters: Alibaba Cloud, Tencent Cloud, AWS, and Azure.
- Third-party image repositories: Harbor and JFrog.

Connecting to a Third-party Image Repository

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

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

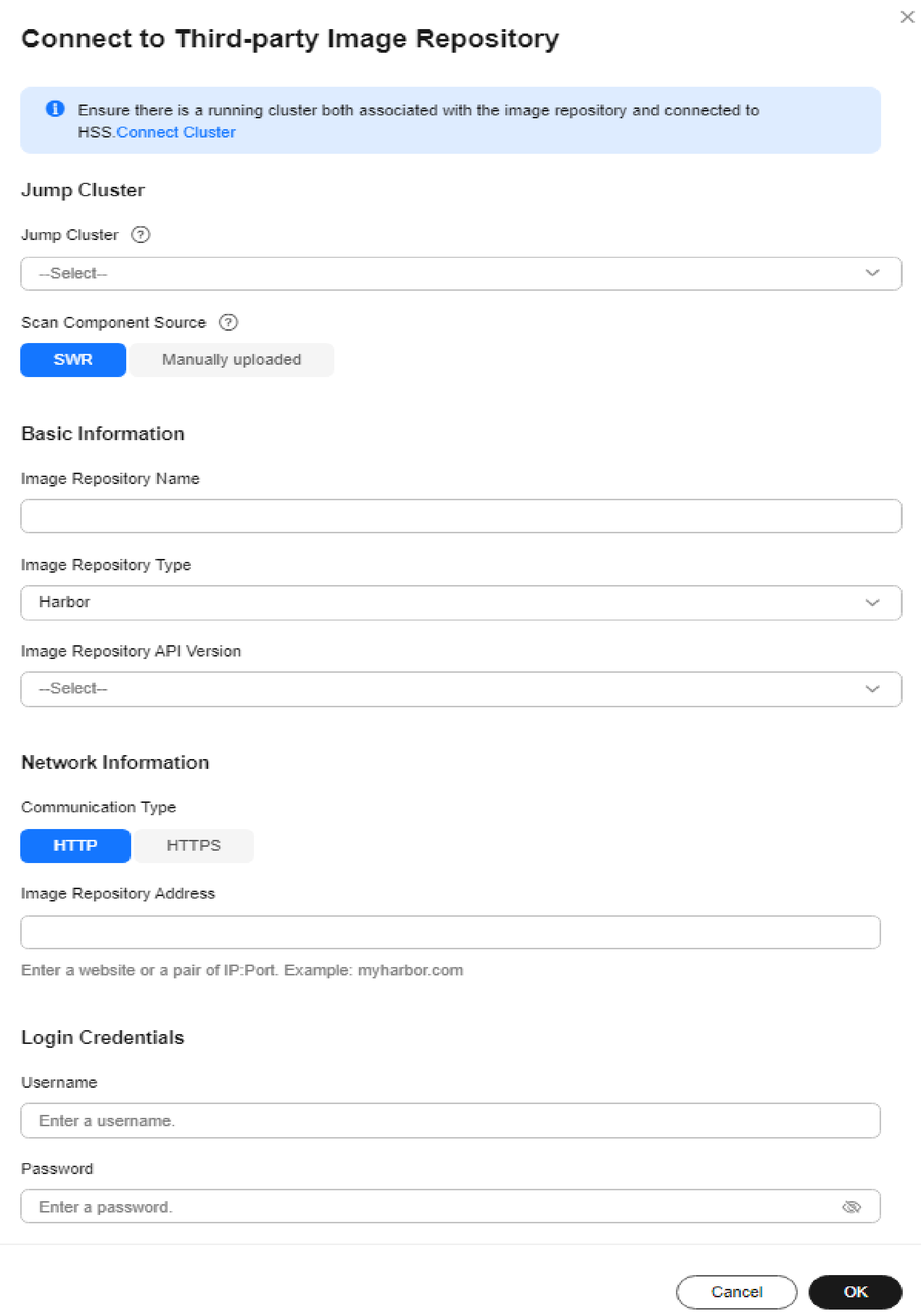
Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **Third-Party Image Repository** tab.

Step 5 Click **Connect to Third-Party Image Repository**.

Step 6 Enter the required information as prompted. For details about the parameters, see **Table 11-18**.

Figure 11-20 Connecting to a Third-party image repository



Connect to Third-party Image Repository

Ensure there is a running cluster both associated with the image repository and connected to HSS.Connect Cluster

Jump Cluster

Jump Cluster: --Select--

Scan Component Source: SWR | Manually uploaded

Basic Information

Image Repository Name

Image Repository Type: Harbor

Image Repository API Version: --Select--

Network Information

Communication Type: HTTP | HTTPS

Image Repository Address

Enter a website or a pair of IP:Port. Example: myharbor.com

Login Credentials

Username: Enter a username.

Password: Enter a password.

Table 11-18 Parameters for accessing an image repository

Parameter	Description	Example Value
Jump Cluster	Select the cluster that carries the image repository.	cluster01
Scan Component Source	The image scan component is used to pull images, scan and analyze required metadata, and transmit the metadata to the server. The server performs security detection on the metadata, such as vulnerabilities, baselines, malicious files, and sensitive information. The image scan component needs to be uploaded to the image repository. You can obtain the image scan component in either of the following ways: ● **SWR**: The cluster can communicate with SWR and obtain image scan components from SWR. ● **Manually uploaded**: If the network between the cluster and SWR is disconnected, you need to manually upload the image scan component to the image repository.	SWR
Image Repository Name	Enter the full name of an image repository.	test
Image Repository Type	Click ⌄ and select the type of the image repository.	Harbor
Image Repository API Version	Click ⌄ and select the interface version of the image repository.	V1
Image Repository Project	If you select **Manually uploaded** and the image repository type is **Harbor**, you need to enter image repository project information.	-

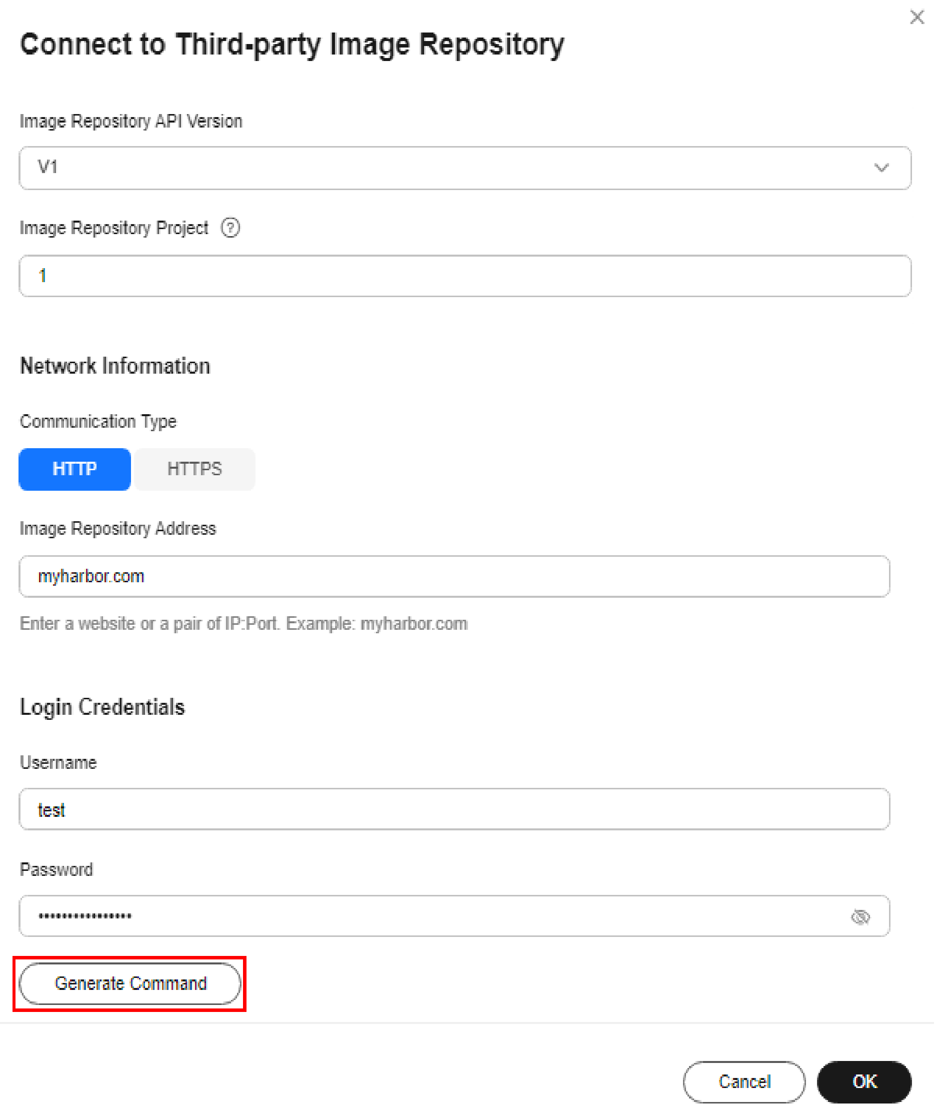
Parameter	Description	Example Value
Image Repository Path	If you select **Manually uploaded** and set the image repository type to **Jfrog**, you need to enter the image repository path.	-
Communication Type	Select the communication protocol type of the image repository. ● **HTTP** ● **HTTPS**	HTTPS
Image Repository Address	Enter the image repository address. You can enter the **website address** or *IP address*:*port number* of the image repository. Example: myharbor.com	myharbor.com
Username	Enter the login username.	-
Password	Enter the password of the login user.	-

Step 7 (Optional) If you select **Manually uploaded** for the scan component, perform the following operations to configure the scan components after entering the access information:

- **For the CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN-Hong Kong, AP-Singapore, CN Southwest-Guiyang1, and AP-Jakarta regions**, **perform the following operations**:

  a. In the **Connect to Third-Party Image Repository** dialog box, click **Generate Command**.

Figure 11-21 Generating a command



Connect to Third-party Image Repository

Image Repository API Version: V1

Image Repository Project: 1

Network Information

Communication Type: HTTP

Image Repository Address: myharbor.com

Enter a website or a pair of IP:Port. Example: myharbor.com

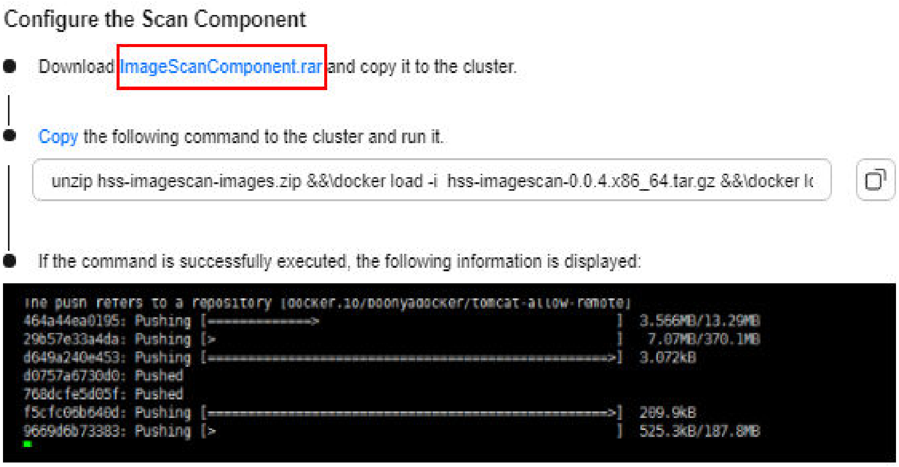
Login Credentials

Username: test

Password: ••••••••••••••••

b. In the **Connect to Third-party Image Repository** dialog box, click **ImageScanComponent.rar** to download the scan component package.

Figure 11-22 Downloading a scan component



Configure the Scan Component

- Download ImageScanComponent.rar and copy it to the cluster.
- Copy the following command to the cluster and run it.

```
unzip hss-imagescan-images.zip &&\docker load -i  hss-imagescan-0.0.4.x86_64.tar.gz &&\docker l(
```

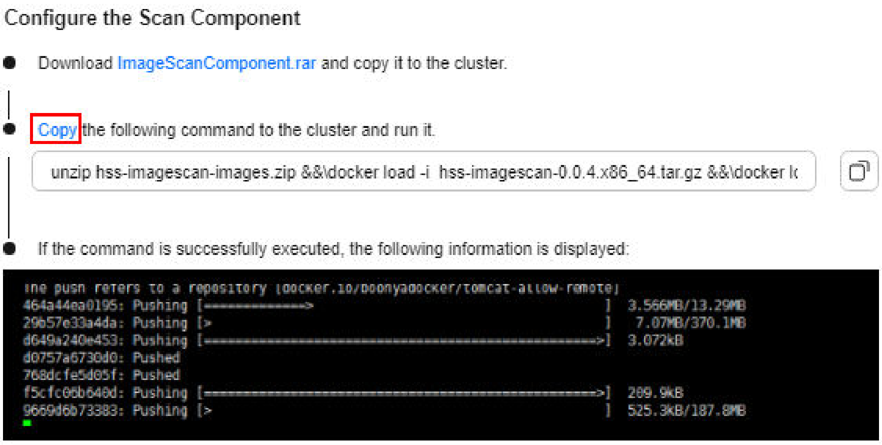
- If the command is successfully executed, the following information is displayed:

```
The push refers to a repository [docker.io/boonyadocker/tomcat-allow-remote]
464a44ea0195: Pushing [=============>                                     ]  3.566MB/13.29MB
29b57e33a4da: Pushing [>                                                  ]   7.07MB/370.1MB
d649a240e453: Pushing [==================================================>]  3.072kB
d0757a6730d0: Pushed
768dcfe5d05f: Pushed
f5cfc06b640d: Pushing [==================================================>]  209.9kB
9669d6b73383: Pushing [>                                                  ]  525.3kB/187.8MB
```

c. Copy the **ImageScanComponent.rar** to any cluster node.

d. In the **Connect to Third-party Image Repository** dialog box, click **Copy the following command**. Run the copied command on the cluster node where **ImageScanComponent.rar** is located. The scan component will be uploaded to the image repository.

Figure 11-23 Copying a command



Configure the Scan Component

- Download ImageScanComponent.rar and copy it to the cluster.
- Copy the following command to the cluster and run it.

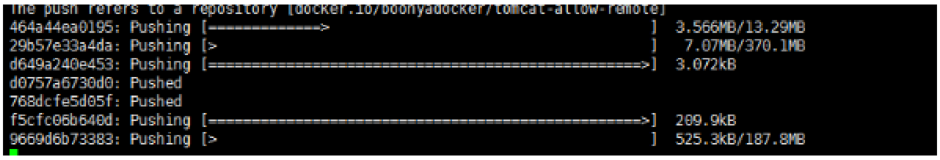
```
unzip hss-imagescan-images.zip &&\docker load -i  hss-imagescan-0.0.4.x86_64.tar.gz &&\docker l(
```

- If the command is successfully executed, the following information is displayed:

```
The push refers to a repository [docker.io/boonyadocker/tomcat-allow-remote]
464a44ea0195: Pushing [=============>                                     ]  3.566MB/13.29MB
29b57e33a4da: Pushing [>                                                  ]   7.07MB/370.1MB
d649a240e453: Pushing [==================================================>]  3.072kB
d0757a6730d0: Pushed
768dcfe5d05f: Pushed
f5cfc06b640d: Pushing [==================================================>]  209.9kB
9669d6b73383: Pushing [>                                                  ]  525.3kB/187.8MB
```

e. If the information shown in **Figure 11-24** is displayed, the scan component is uploaded successfully.

Figure 11-24 Scan component uploaded

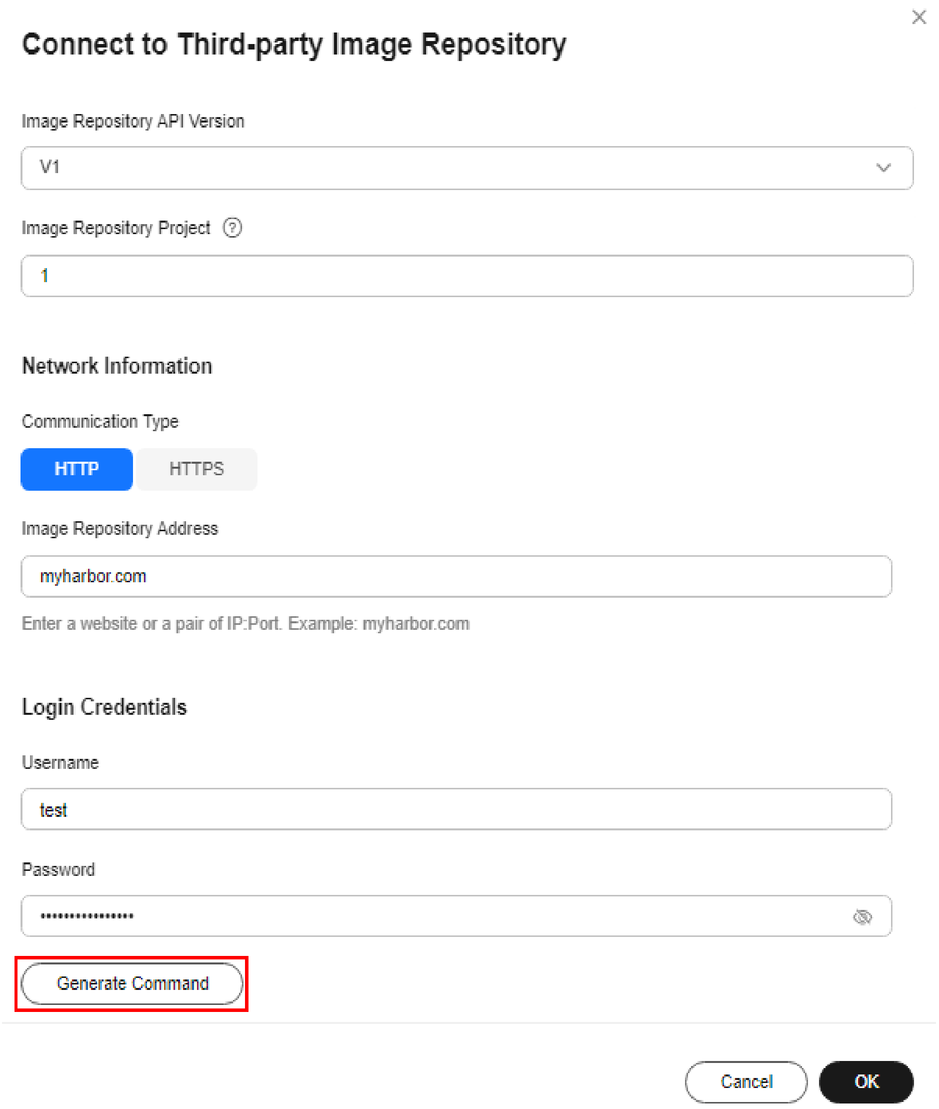


```
The push refers to a repository [docker.io/boonyadocker/tomcat-allow-remote]
464a44ea0195: Pushing [=============>                                     ]  3.566MB/13.29MB
29b57e33a4da: Pushing [>                                                  ]   7.07MB/370.1MB
d649a240e453: Pushing [==================================================>]  3.072kB
d0757a6730d0: Pushed
768dcfe5d05f: Pushed
f5cfc06b640d: Pushing [==================================================>]  209.9kB
9669d6b73383: Pushing [>                                                  ]  525.3kB/187.8MB
```

- **For other regions, perform the following operations:**

a. In the **Connect to Third-Party Image Repository** dialog box, click **Generate Command**.

Figure 11-25 Generating commands



Connect to Third-party Image Repository

Image Repository API Version: V1

Image Repository Project: 1

Network Information

Communication Type: HTTP

Image Repository Address: myharbor.com

Enter a website or a pair of IP:Port. Example: myharbor.com

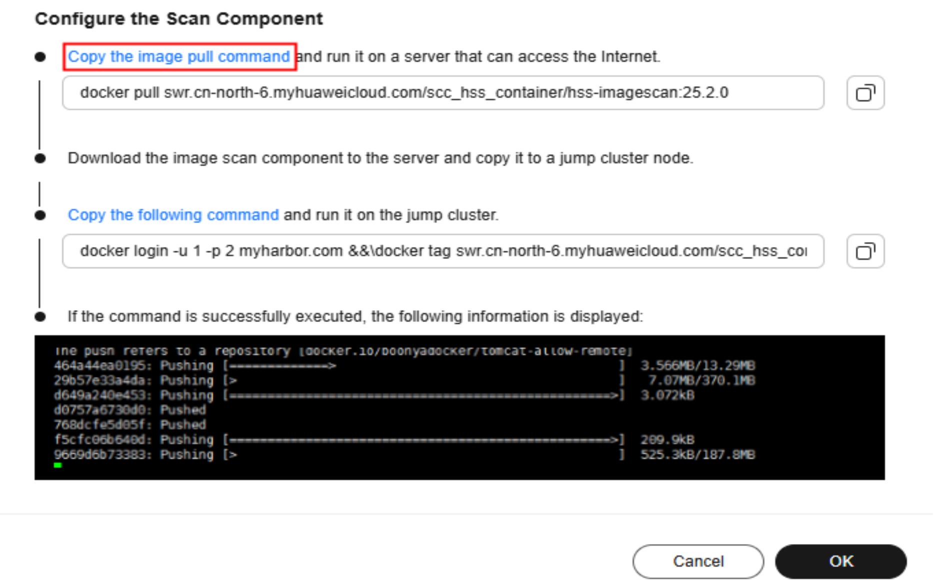
Login Credentials

Username: test

Password: ••••••••••••••••

b. In the **Connect to Third-party Image Repository** dialog box, click **Copy the image pull command**.

Figure 11-26 Downloading a scan component



Configure the Scan Component

- Copy the image pull command and run it on a server that can access the Internet.

```
docker pull swr.cn-north-6.myhuaweicloud.com/scc_hss_container/hss-imagescan:25.2.0
```

- Download the image scan component to the server and copy it to a jump cluster node.
- Copy the following command and run it on the jump cluster.

```
docker login -u 1 -p 2 myharbor.com &&\docker tag swr.cn-north-6.myhuaweicloud.com/scc_hss_coı
```

- If the command is successfully executed, the following information is displayed:

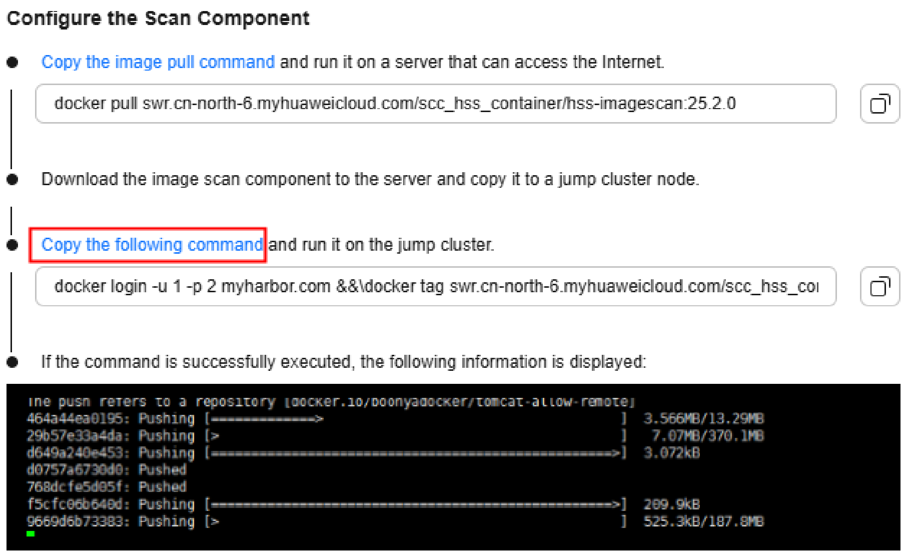
```
The push refers to a repository [docker.io/boonyadocker/tomcat-allow-remote]
464a44ea0195: Pushing [=============>                                     ]  3.566MB/13.29MB
29b57e33a4da: Pushing [>                                                  ]   7.07MB/370.1MB
d649a240e453: Pushing [==================================================>]  3.072kB
d0757a6730d0: Pushed
768dcfe5d05f: Pushed
f5cfc06b640d: Pushing [==================================================>]  209.9kB
9669d6b73383: Pushing [>                                                  ]  525.3kB/187.8MB
```

c. Log in to any Linux server that can access the Internet, paste and run the command copied in **Step 7.b** to download the scan component image.

d. Copy the downloaded scan component image to any node in the repository cluster.

e. In the **Connect to Third-party Image Repository** dialog box, click **Copy the following command**. Run the copied command on the cluster node where the scan component is located. The scan component will be uploaded to the image repository.

Figure 11-27 Copying commands



Configure the Scan Component

- Copy the image pull command and run it on a server that can access the Internet.

```
docker pull swr.cn-north-6.myhuaweicloud.com/scc_hss_container/hss-imagescan:25.2.0
```

- Download the image scan component to the server and copy it to a jump cluster node.
- Copy the following command and run it on the jump cluster.

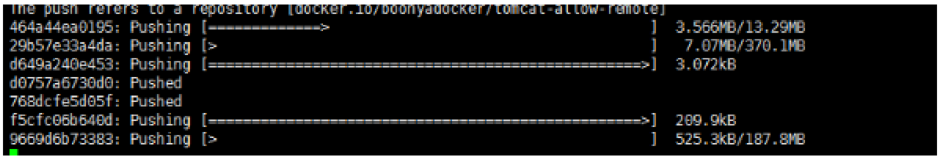
```
docker login -u 1 -p 2 myharbor.com &&\docker tag swr.cn-north-6.myhuaweicloud.com/scc_hss_coı
```

- If the command is successfully executed, the following information is displayed:

```
The push refers to a repository [docker.io/boonyadocker/tomcat-allow-remote]
464a44ea0195: Pushing [=============>                                     ]  3.566MB/13.29MB
29b57e33a4da: Pushing [>                                                  ]   7.07MB/370.1MB
d649a240e453: Pushing [==================================================>]  3.072kB
d0757a6730d0: Pushed
768dcfe5d05f: Pushed
f5cfc06b640d: Pushing [==================================================>]  209.9kB
9669d6b73383: Pushing [>                                                  ]  525.3kB/187.8MB
```

f. If the information shown in **Figure 11-28** is displayed, the scan component is uploaded successfully.

Figure 11-28 Scan component uploaded



```
The push refers to a repository [docker.io/boonyadocker/tomcat-allow-remote]
464a44ea0195: Pushing [=============>                                     ]  3.566MB/13.29MB
29b57e33a4da: Pushing [>                                                  ]   7.07MB/370.1MB
d649a240e453: Pushing [==================================================>]  3.072kB
d0757a6730d0: Pushed
768dcfe5d05f: Pushed
f5cfc06b640d: Pushing [==================================================>]  209.9kB
9669d6b73383: Pushing [>                                                  ]  525.3kB/187.8MB
```

Step 8 Click **OK** to connect to the image repository.

Step 9 On the **Third-party Image Repositories** tab page, view the access result in the **Image Repository Status** column of the target image repository.

----End

11.8 CI/CD Image Access Configuration

11.8.1 Accessing CI/CD

Scenario

Integrate the image security scan plug-in of HSS in the Jenkins Pipeline project so that images can be scanned during the Jenkins Pipeline project construction.

Prerequisite

You have enabled the **pay-per-use CI/CD image scan**. You will be paid per image per scan. For details, see **Enabling Pay-per-use Container Image Scan**.

Accessing CI/CD

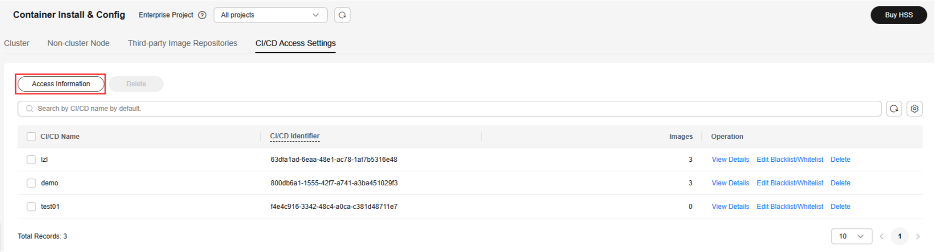
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **CI/CD Access Settings** tab and then click **Access Information**.

Figure 11-29 CI/CD access settings



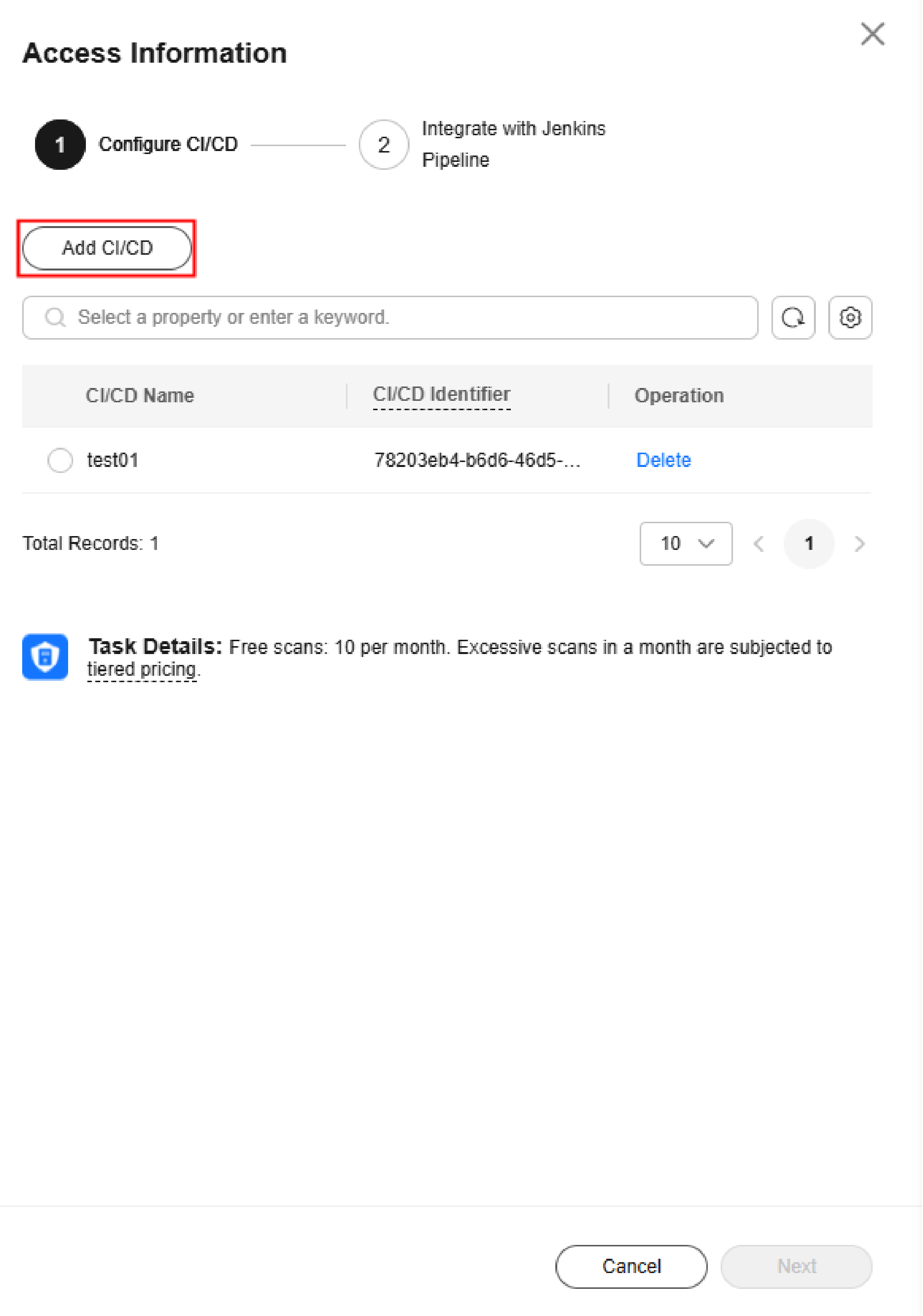
CI/CD Name	CI/CD Identifier	Images	Operation
lzl	63dfa1ad-6eaa-48e1-ac78-1af7b5316e48	3	View Details Edit Blacklist/Whitelist Delete
demo	800db6a1-1555-42f7-a741-a3ba451029f3	3	View Details Edit Blacklist/Whitelist Delete
test01	f4e4c916-3342-48c4-a0ca-c381d48711e7	0	View Details Edit Blacklist/Whitelist Delete

Total Records: 3

Step 5 In the dialog box that is displayed, click **Add CI/CD**.

The CI/CD identifier is the access token of the CI/CD plug-in and is used for identity authentication during image scans.

Figure 11-30 Adding CI/CD



Access Information

1 Configure CI/CD — 2 Integrate with Jenkins Pipeline

Add CI/CD

Select a property or enter a keyword.

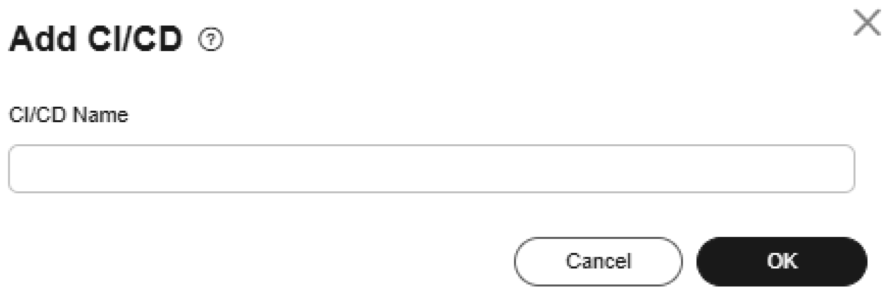
	CI/CD Name	CI/CD Identifier	Operation
○	test01	78203eb4-b6d6-46d5-...	Delete

Total Records: 1

Task Details: Free scans: 10 per month. Excessive scans in a month are subjected to tiered pricing.

Step 6 Enter an identifier and click **OK**. The CI/CD identifier is added.

Figure 11-31 Entering an CI/CD identifier

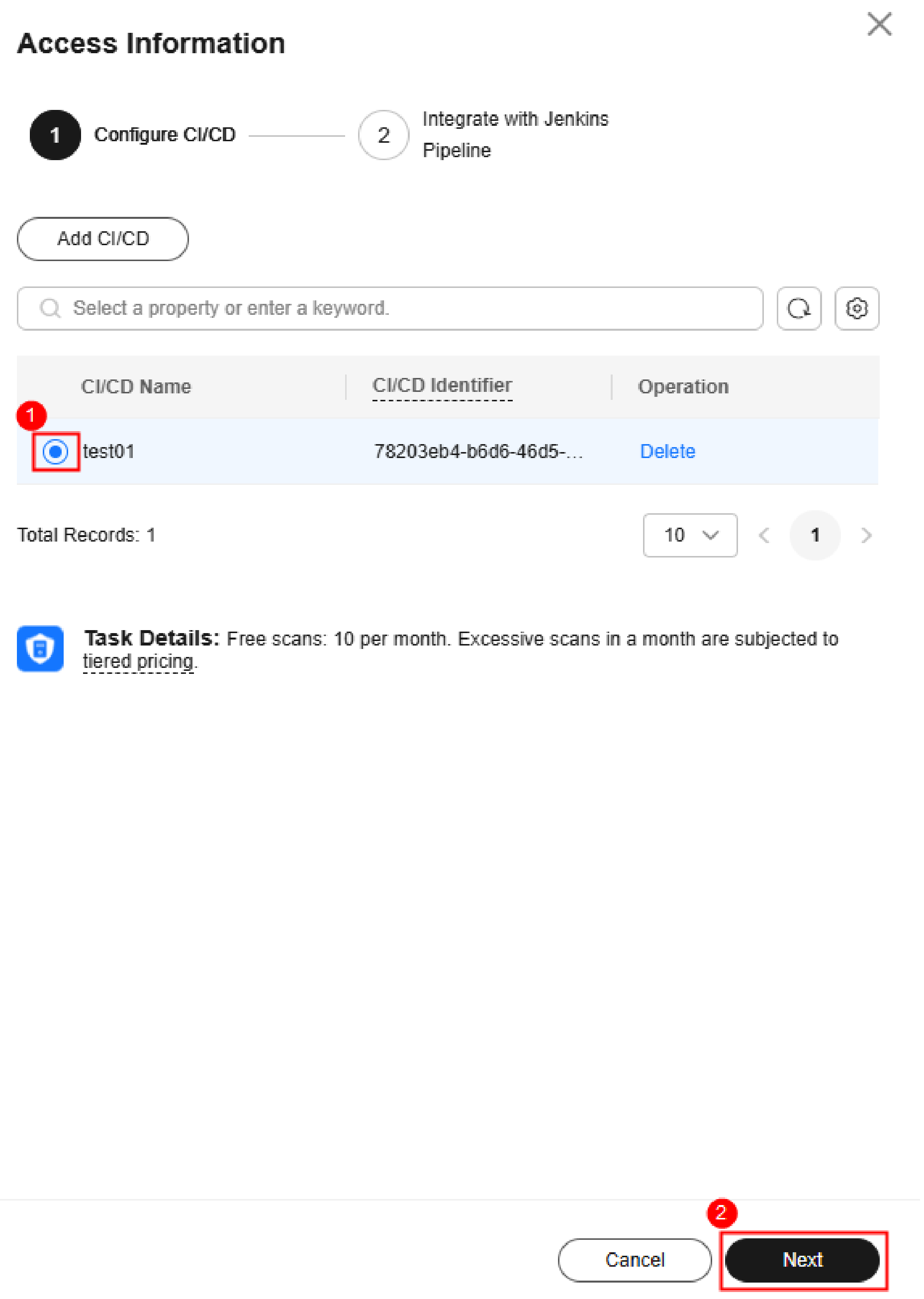


Add CI/CD

CI/CD Name

Step 7 Select an identifier and click **Next**.

Figure 11-32 Selecting an identifier



Access Information

1 Configure CI/CD
2 Integrate with Jenkins Pipeline
Add CI/CD
Select a property or enter a keyword.

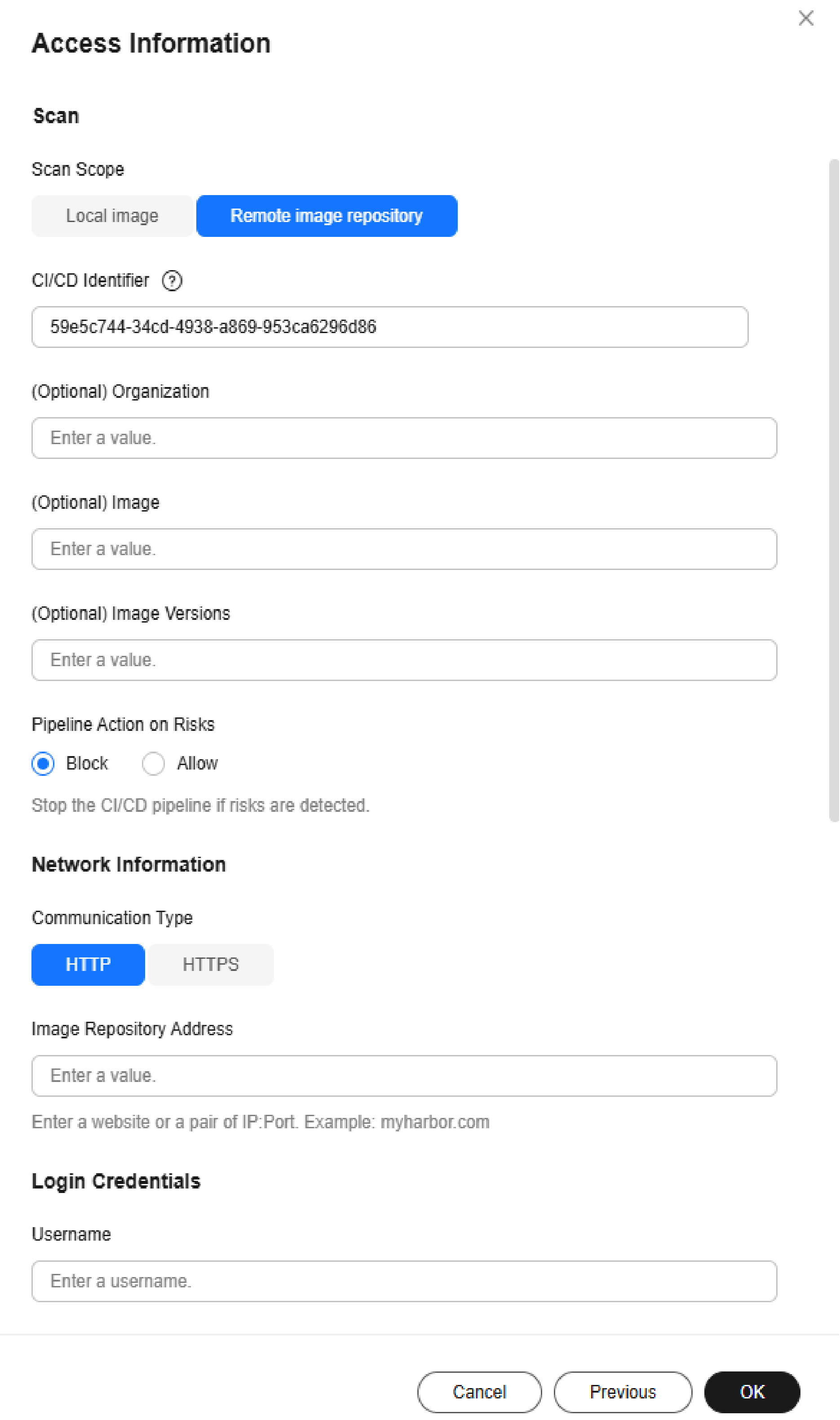
CI/CD Name	CI/CD Identifier	Operation
● test01	78203eb4-b6d6-46d5-...	Delete

Total Records: 1

Task Details: Free scans: 10 per month. Excessive scans in a month are subjected to tiered pricing.

Step 8 Configure image scan information as prompted.

Figure 11-33 Image scan information



Access Information

Scan

Scan Scope: Local image / Remote image repository (selected)

CI/CD Identifier: 59e5c744-34cd-4938-a869-953ca6296d86

(Optional) Organization: Enter a value.

(Optional) Image: Enter a value.

(Optional) Image Versions: Enter a value.

Pipeline Action on Risks: ● Block ○ Allow

Stop the CI/CD pipeline if risks are detected.

Network Information

Communication Type: HTTP (selected) / HTTPS

Image Repository Address: Enter a value.

Enter a website or a pair of IP:Port. Example: myharbor.com

Login Credentials

Username: Enter a username.

Table 11-19 Image scan parameters

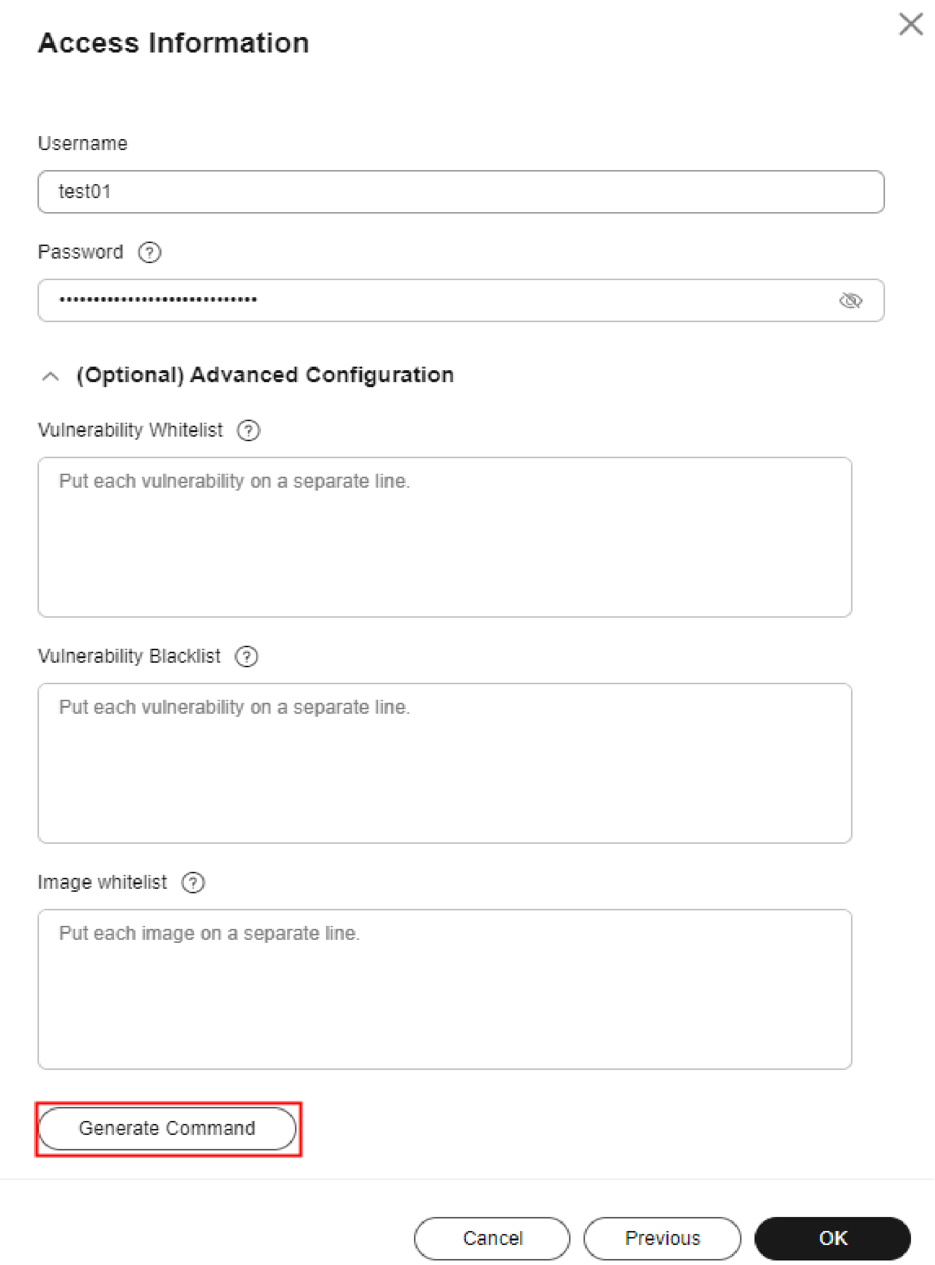
Category	Parameter on GUI	Description	Parameter in Command
Scan	Scan Scope	Type of images to be scanned. ● **Local image** ● **Remote image repository**	-
	CI/CD Identifier	CI/CD plug-in access token used for identity authentication during image scans.	cicd_id
	(Optional) Organization	If **Scan Scope** is set to **Remote image repository**, you can enter the name of the organization that the remote image belongs to.	NAMESPACE
	(Optional) Image	Image name.	IMAGE_NAME
	(Optional) Image Versions	Image version information.	IMAGE_VERSION
	Pipeline Action on Risks	HSS will handle insecure images during image building based on the selected action. ● Block: When high-risk images are detected, the CI/CD pipeline is blocked. High-risk images refer to the images whose risk level is high in the check results of vulnerabilities, malicious files, or baselines. ● Allow: The CI/CD pipeline is allowed to run properly even if image risks are detected.	is_blocking ● Blocking the pipeline: **is_blocking=1** ● Allowing the pipeline: **is_blocking=0** To block all the insecure pipelines, including the pipelines with high-risk images, set **is_blocking=non-secure**.

Category	Parameter on GUI	Description	Parameter in Command
Network Information (required only for remote image repository scans)	Communication Type	Communication protocol type of the image repository. - **HTTP** - **HTTPS**	repository_address Value format: *Communication_type*://*Image_repository_address*
	Image Repository Address	Image repository address. You can enter the website address or *IP_address*:*Port_number* of the image repository. Example: **myharbor.com**	repository_address Value format: *Communication_type*://*Image_repository_address*
Login Credentials (required only for remote image repository scans)	Username	Login username.	login_auth The value of this parameter is the encrypted value of the **image repository username** and **image repository password**.
	Password	Password of the login user.	login_auth The value of this parameter is the encrypted value of the **image repository username** and **image repository password**.

Category	Parameter on GUI	Description	Parameter in Command
(Optional) Advanced Configuration	Vulnerability Whitelist	During CI/CD pipeline building, if an image only has whitelist vulnerabilities, the CI/CD pipeline is not blocked. If you believe a high-risk vulnerability does not affect your services, you can add it to the vulnerability whitelist. Enter one or multiple vulnerability names. Put each vulnerability name on a separate line.	-
	Vulnerability Blacklist	During CI/CD pipeline building, if an image has a blacklisted vulnerability, the CI/CD pipeline is blocked. If you believe a low-risk vulnerability severely affects your services, you can add it to the vulnerability blacklist. Enter one or multiple vulnerability names. Put each vulnerability name on a separate line.	-
	Image Whitelist	During CI/CD pipeline building, if the image is found to have risks, the CI/CD pipeline is not blocked. Enter one or multiple image names. Put each image name on a separate line. Image name format: ● Local image: *Image_name*:*Version* ● Remote image: *Organization_name*/*Image_name*:*Version*	-

Step 9 After the configuration is complete, click **Generate Command** to generate commands for configuring the image security scan plug-in.

Figure 11-34 Generating commands



Access Information

Username

test01

Password

••••••••••••••••••••••••••••••

(Optional) Advanced Configuration

Vulnerability Whitelist

Put each vulnerability on a separate line.

Vulnerability Blacklist

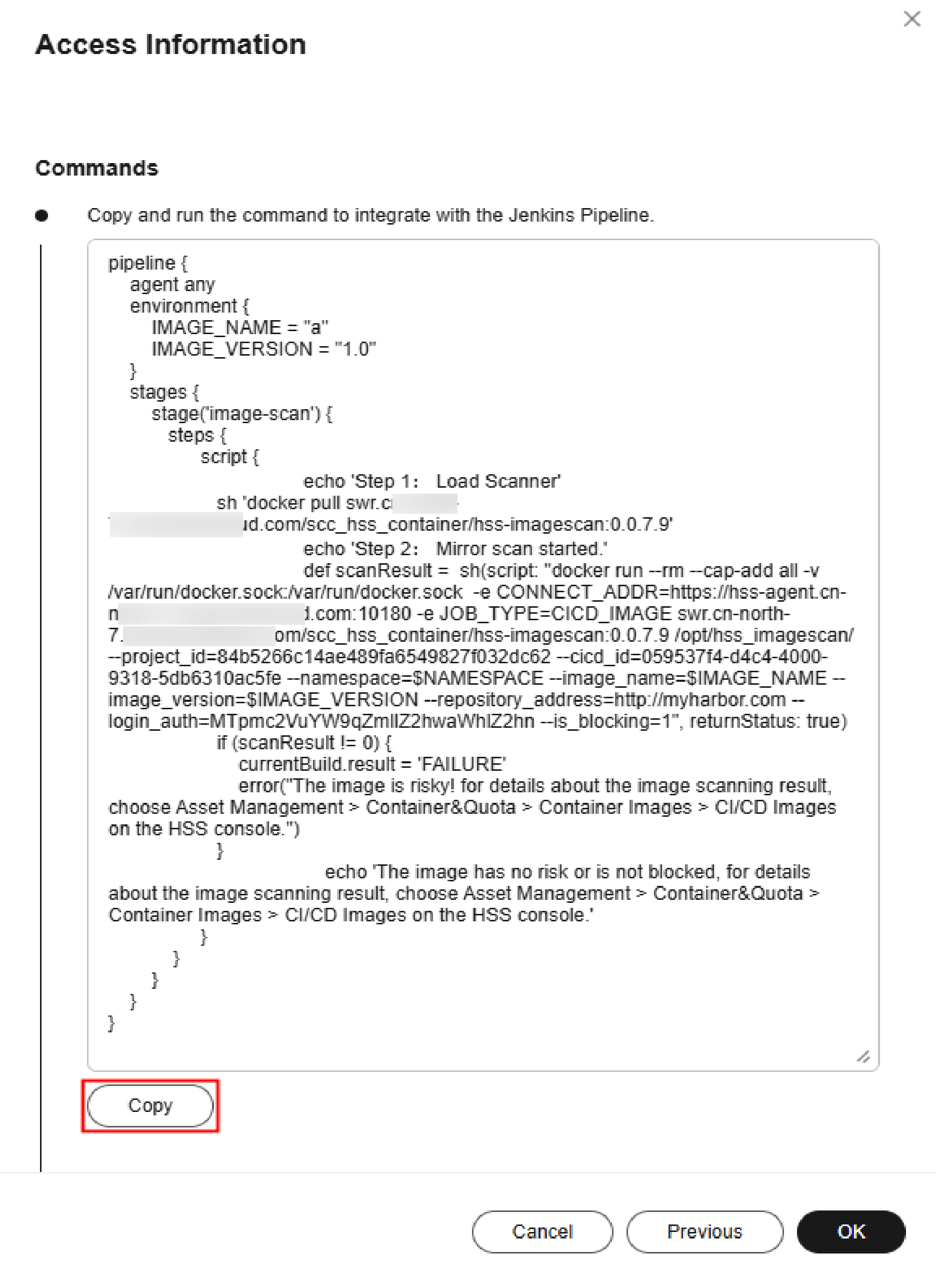
Put each vulnerability on a separate line.

Image whitelist

Put each image on a separate line.

Step 10 Click **Copy**, as shown in **Figure 11-35**.

Figure 11-35 Copying commands



Commands

- Copy and run the command to integrate with the Jenkins Pipeline.

```
pipeline {
   agent any
   environment {
      IMAGE_NAME = "a"
      IMAGE_VERSION = "1.0"
   }
   stages {
      stage('image-scan') {
         steps {
             script {
                           echo 'Step 1:   Load Scanner'
               sh 'docker pull swr.c[redacted]
[redacted]ud.com/scc_hss_container/hss-imagescan:0.0.7.9'
                           echo 'Step 2:   Mirror scan started.'
                           def scanResult =  sh(script: "docker run --rm --cap-add all -v
/var/run/docker.sock:/var/run/docker.sock  -e CONNECT_ADDR=https://hss-agent.cn-
n[redacted]d.com:10180 -e JOB_TYPE=CICD_IMAGE swr.cn-north-
7.[redacted]om/scc_hss_container/hss-imagescan:0.0.7.9 /opt/hss_imagescan/
--project_id=84b5266c14ae489fa6549827f032dc62 --cicd_id=059537f4-d4c4-4000-
9318-5db6310ac5fe --namespace=$NAMESPACE --image_name=$IMAGE_NAME --
image_version=$IMAGE_VERSION --repository_address=http://myharbor.com --
login_auth=MTpmc2VuYW9qZmllZ2hwaWhlZ2hn --is_blocking=1", returnStatus: true)
               if (scanResult != 0) {
                  currentBuild.result = 'FAILURE'
                  error("The image is risky! for details about the image scanning result,
choose Asset Management > Container&Quota > Container Images > CI/CD Images
on the HSS console.")
               }
                              echo 'The image has no risk or is not blocked, for details
about the image scanning result, choose Asset Management > Container&Quota >
Container Images > CI/CD Images on the HSS console.'
             }
         }
      }
   }
}
```

Step 11 Log in to Jenkins.

Step 12 On the **Dashboard** page, click the name of a project in Jenkins-Pipeline mode.

In this example, the project name is **mypipeline**.

Step 13 In the navigation tree on the left, choose **Configure**.

Step 14 Insert image security scan commands based on the type of the images to be scanned.

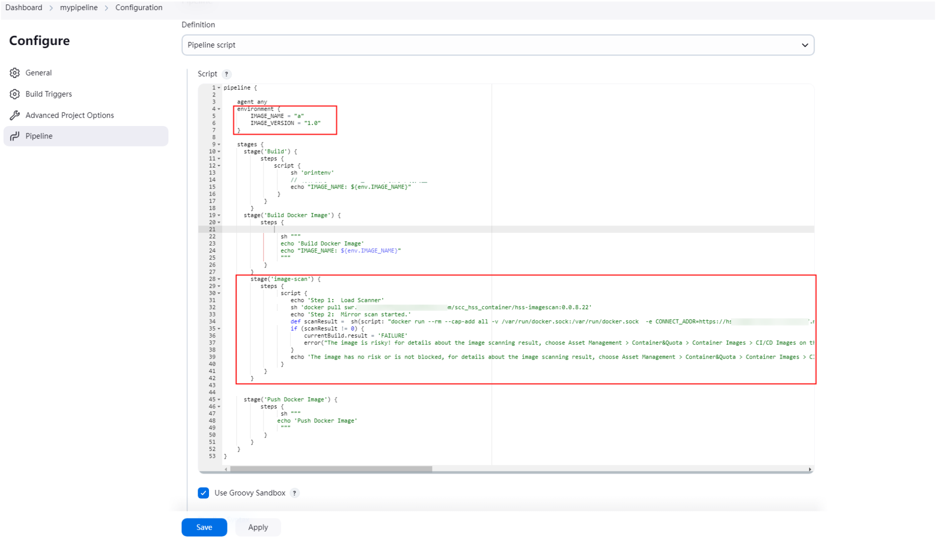
The following example is for reference only.

- **Local images**

1. In the **Pipeline** area, insert the **environment** code segment of the command copied in **Step 10** after **agent any** in the pipeline script.

2. Insert the **stage('image-scan')** code segment of the command copied in **Step 10** between the Build and Push phases in the pipeline script.

Figure 11-36 Inserting image security scan commands



```
pipeline {

    agent any
    environment {
        IMAGE_NAME = "a"
        IMAGE_VERSION = "1.0"
    }

    stages {
      stage('Build') {
          steps {
              script {
                   sh 'printenv'
                   //
                   echo "IMAGE_NAME: ${env.IMAGE_NAME}"
              }
          }
      }
      stage('Build Docker Image') {
          steps {

                 sh """
                 echo 'Build Docker Image'
                 echo "IMAGE_NAME: ${env.IMAGE_NAME}"
                 """
          }
      }
        stage('image-scan') {
          steps {
                 script {
                   echo 'Step 1:  Load Scanner'
                   sh 'docker pull swr.[redacted]m/scc_hss_container/hss-imagescan:0.0.8.22'
                   echo 'Step 2:  Mirror scan started.'
                   def scanResult =  sh(script: "docker run --rm --cap-add all -v /var/run/docker.sock:/var/run/docker.sock  -e CONNECT_ADDR=https://hs[redacted]'.r
                   if (scanResult != 0) {
                       currentBuild.result = 'FAILURE'
                       error("The image is risky! for details about the image scanning result, choose Asset Management > Container&Quota > Container Images > CI/CD Images on th
                   }
                   echo 'The image has no risk or is not blocked, for details about the image scanning result, choose Asset Management > Container&Quota > Container Images > C
                 }
          }
        }


      stage('Push Docker Image') {
          steps {
                 sh """
                echo 'Push Docker Image'
                 """
          }
      }
    }
}
```

☑ Use Groovy Sandbox ?

- **Remote image repository**
  a. In the **Pipeline** area, insert the **environment** code segment of the command copied in **Step 10** after **agent any** in the pipeline script.
  b. Insert the **stage('image-scan')** code segment of the command copied in **Step 10** between the Test and Push phases in the pipeline script.

Step 15 Click **Apply**.

Image security scan tasks will be executed while you build the project.

You can use **Blue Ocean** to view the project build task. Image security scan is performed in the **image-Scan** step added to the project. After the scan is complete, you can view its results on the HSS console. For details, see **Viewing and Handling CI/CD Image Scan Results**.

If you choose to block a pipeline while performing **Step 8**, the image security scan plug-in will block the pipeline having high-risk images, as shown in **Figure 11-37**.

Figure 11-37 Blocking project building

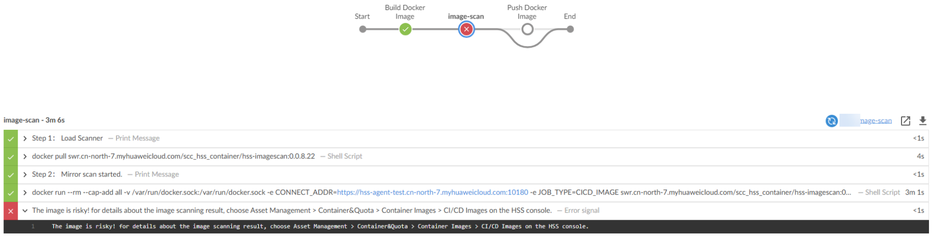


image-scan - 3m 6s

```
✓ > Step 1:  Load Scanner  — Print Message    <1s
✓ > docker pull swr.cn-north-7.myhuaweicloud.com/scc_hss_container/hss-imagescan:0.0.8.22  — Shell Script    4s
✓ > Step 2:  Mirror scan started.  — Print Message    <1s
✓ > docker run --rm --cap-add all -v /var/run/docker.sock:/var/run/docker.sock -e CONNECT_ADDR=https://hss-agent-test.cn-north-7.myhuaweicloud.com:10180 -e JOB_TYPE=CICD_IMAGE swr.cn-north-7.myhuaweicloud.com/scc_hss_container/hss-imagescan:0...  — Shell Script   3m 1s
✕ ⌄ The image is risky! for details about the image scanning result, choose Asset Management > Container&Quota > Container Images > CI/CD Images on the HSS console.  — Error signal    <1s
    1    The image is risky! for details about the image scanning result, choose Asset Management > Container&Quota > Container Images > CI/CD Images on the HSS console.
```

----End

Related Operations

- **Viewing and Handling CI/CD Image Scan Results**

- **Editing the Blacklist or Whitelist**

11.8.2 Editing the Blacklist or Whitelist

Scenario

The blacklist and whitelist can control image blocking during image building. They can be configured during CI/CD access. This section describes how to add or modify blacklist or whitelist items after the CI/CD access configuration is complete.

Editing the Blacklist or Whitelist

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

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

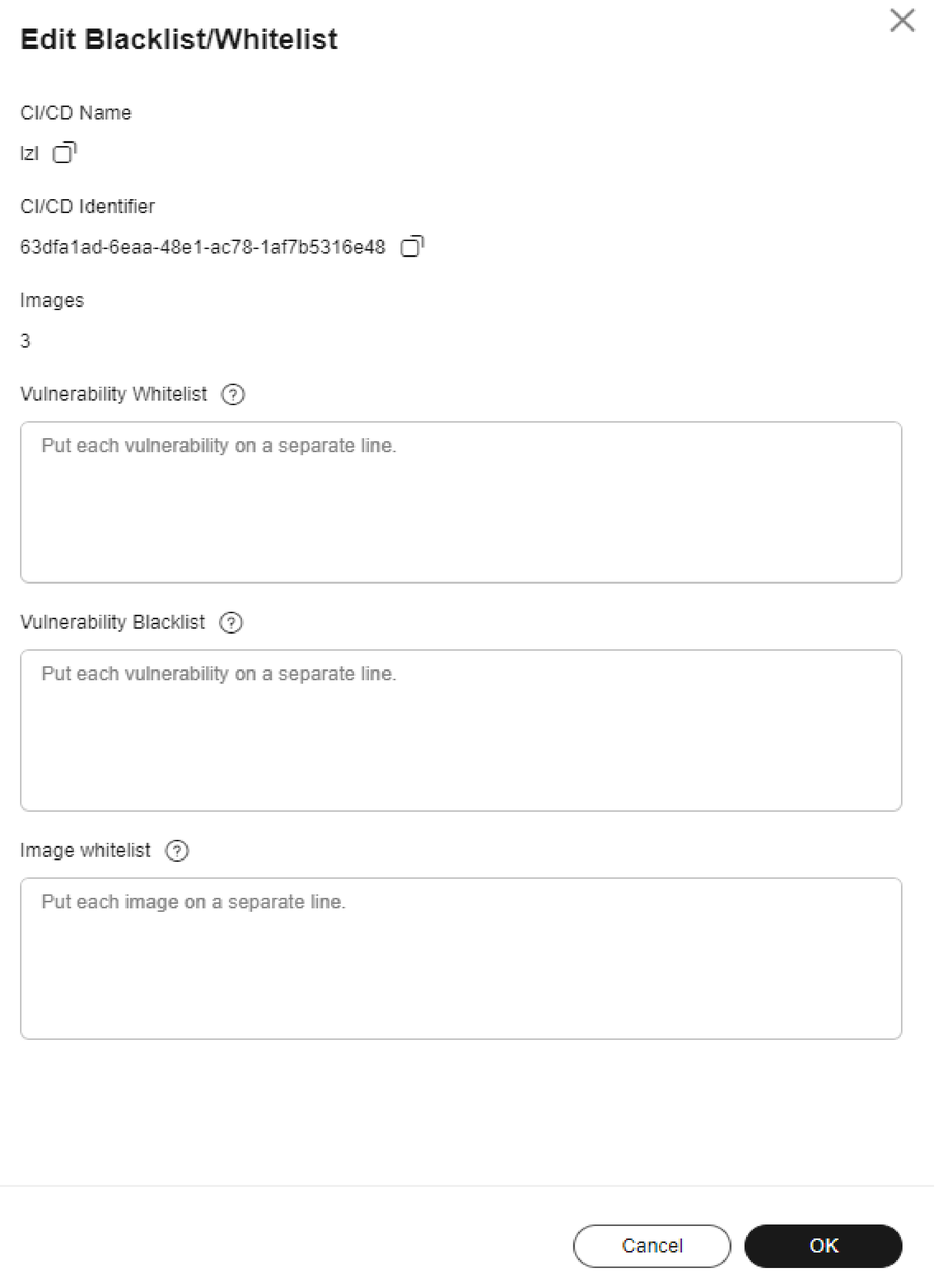
Step 3 In the navigation pane, choose **Installation & Configuration** > **Container Install & Config**.

Step 4 Click the **CI/CD Access Settings** tab.

Step 5 In the row of a CI/CD identifier, click **Edit Blacklist/Whitelist** in the **Operation** column.

Step 6 In the slide-out panel that is displayed, edit the vulnerability whitelist, vulnerability blacklist, and image whitelist.

Figure 11-38 Editing the blacklist or whitelist



Edit Blacklist/Whitelist

CI/CD Name

lzl

CI/CD Identifier

63dfa1ad-6eaa-48e1-ac78-1af7b5316e48

Images

3

Vulnerability Whitelist

Put each vulnerability on a separate line.

Vulnerability Blacklist

Put each vulnerability on a separate line.

Image whitelist

Put each image on a separate line.

Table 11-20 Blacklist and whitelist parameters

Parameter	Description
Vulnerability Whitelist	During CI/CD pipeline building, if an image only has whitelist vulnerabilities, the CI/CD pipeline is not blocked. If you believe a high-risk vulnerability does not affect your services, you can add it to the vulnerability whitelist. Enter one or multiple vulnerability names. Put each vulnerability name on a separate line. You can remove a vulnerability from the whitelist.
Vulnerability Blacklist	During CI/CD pipeline building, if an image has a blacklisted vulnerability, the CI/CD pipeline is blocked. If you believe a low-risk vulnerability severely affects your services, you can add it to the vulnerability blacklist. Enter one or multiple vulnerability names. Put each vulnerability name on a separate line. You can remove a vulnerability from the blacklist.
Image Whitelist	During CI/CD pipeline building, if the image is found to have risks, the CI/CD pipeline is not blocked. Enter one or multiple image names to add them to the whitelist. Put each image name on a separate line. Image name format: ● Local image: *Image_name*:*Version* ● Remote image: *Organization_name*/*Image_name*:*Version* You can remove an image from the whitelist.

Step 7 After the editing is complete, click **OK**.

----End

12 Account Management

12.1 Account Management Overview

HSS can collect statistics on the servers and risks under your organization member accounts. If your account is managed by an organization, you can view the number of servers under all the member accounts in the organization, as well as the number of vulnerabilities, baselines, and alarms of the servers.

To use HSS to view the numbers of servers and risks under your organization member accounts in a unified manner, perform the following operations:

1. **Adding an Account to an Organization**
2. **Viewing Account Management**

For details about the organization service, see **Overview of Organizations**.

12.2 Adding an Account to an Organization

To use HSS to view the numbers of servers and risks under your organization member accounts in a unified manner, perform the operations in this section to add accounts first.

Prerequisites

- You have created an organization. For details, see **Creating an Organization**.
- You have configured HSS as a trusted service. For details, see **Enabling or Disabling a Trusted Service**.
- The current account is the organization administrator or the delegated administrator. For more information, see **Adding a Delegated Administrator**.

Adding an Account to an Organization

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

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

Step 3 In the navigation pane on the left, choose **Installation & Configuration** and click the **Account Management** tab. On the displayed page, click **Add Account**.

Step 4 On the dialog box that is displayed, select an account from the **Available Accounts** tree. The account is automatically added to the **Selected Accounts** area on the right. Confirm the information and click **OK**.

NOTE

The added accounts belong to the same organization. For details about organization accounts, see **Overview of an Account**.

Step 5 The account is added successfully and is displayed in the account list.

----End

12.3 Viewing Security Risks of Organization Member Accounts

After organization member accounts are added to HSS, you can view the risks of these accounts on the **Account Management** page.

Viewing Security Risks of Organization Member Accounts

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

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

Step 3 In the navigation pane on the left, choose **Installation & Configuration** and click the **Account Management** tab. On the displayed page, view the list of all accounts. For more information, see **Parameter description**.

Table 12-1 Parameter description

Parameter	Description
Account Name	Account name
Project Name	Region to which the account belongs
Servers	Number of servers under an account
Vulnerabilities (Last 24 hours)	Number of vulnerabilities on servers in the last 24 hours
Unsafe Settings (Last 24 hours)	Number of unsafe settings on servers in the last 24 hours
Alarms (Last 24 hours)	Number of security alarms on servers in the last 24 hours

----End

Deleting an Account

Step 1 Click **Delete** in the **Operation** column of the target account.

Step 2 In the dialog box that is displayed, confirm the information and click **OK**.

----End

13 Plug-in Settings

13.1 Plug-Ins Overview

If container protection is enabled and you want to use the image blocking function, you need to **install the Docker plug-in**.

The Docker plug-in provides the image blocking capability. It can prevent the startup of container images that have high-risk vulnerabilities or do not comply with security standards in the Docker environment.

You can configure image blocking in the following scenarios:

- To enhance the security of container images and prevent the risks caused by the use of untrusted or outdated images, you can configure an **image blocking policy** to specify the level of vulnerabilities to be blocked or the whitelist.
- If you need to comply with the security requirements of certain industries or regulations, such as PCI DSS and CIS, you can **configure an image blocking policy** to specify the security baseline or compliance check items to be blocked.
- If you need to implement the best practices of container DevSecOps and embed security check and defense into each phase of the container lifecycle, you can **configure an image blocking policy** to enhance security from source to devices.

Constraints

The constraints for installing the Docker plug-in are as follows:

- The HSS container edition has been enabled.
- Only Docker containers can use this plug-in.
- The Docker engine version is 18.06.0 or later.
- The Docker API version is 1.38 or later.
- Only Linux servers are supported.
- Only the x86 and Arm hardware architectures are supported.

- Currently, this plug-in can be installed only on Huawei Cloud servers.

13.2 Viewing Plug-in Information

The plug-in configuration page displays the server list and the plug-in information of the servers. If no plug-ins are installed on a server, the corresponding plug-in information is empty. You can view the plug-in information of a server to determine the servers where plug-ins need to be installed.

Viewing Plug-in Information

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Installation & Configuration** > **Plug-in Settings**. View plug-in details on the plug-in settings page. For more information, see **Table 13-1**.

By default, all servers are displayed in the plug-in list. If a plug-in is installed on a server, the plug-in details are displayed. If no plug-ins are installed on a server, the plug-in information is empty.

Table 13-1 Docker plug-in list parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	Server IP address
OS	Type of the OS running on the server
Plug-in Name	Name of the plug-in installed on the server.
Plug-in Version	Name of the plug-in installed on the server.
Plug-in Status	Current status of the plug-in. ● **Created**: The plug-in has been created but has not been started. ● **Running**: The plug-in is running properly. ● **Paused**: The plug-in is paused. ● **Restarting**: The plug-in is being restarted. ● **Removing**: The plug-in is being deleted. ● **Exited**: The plug-in has been stopped. ● **Dead**: The plug-in cannot be started or has been deleted.

Parameter	Description
Plug-in Upgrade Status	Plug-in upgrade status. ● **Not upgraded**: The plug-in has not been upgraded to the latest version. ● **Upgrading**: The plug-in is being upgraded. ● **Upgraded**: The plug-in has been upgraded. ● **Upgrade failed**: The plug-in failed to be upgraded.

----End

13.3 Installing a Plug-in

If container protection is enabled and you want to use the image blocking function, install the Docker plug-in by following the instructions provided in this section.

Installing a Plug-in

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Installation & Configuration** > **Plug-in Settings**. Click **Plug-In Installation Guide**. In the slide-out panel, copy the commands in the **Installation Commands** section.

Step 4 Remotely log in to the server where the plug-in is to be installed as the **root** user.

- Log in to the ECS console, locate the target server, and click **Remote Login** in the **Operation** column to log in to the server. For details, see Login Using VNC.
- If your server has an EIP bound, you can also use a remote management tool, such as PuTTY or Xshell, to log in to the server and install the plug-in on the server as user **root**.

Step 5 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 6 Create **linux-host-list.txt**, which will contain the server private IP addresses where the agent is to be installed:

Command syntax:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
Or
echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

To specify multiple IP addresses, write multiple commands, each in a separate line.

Example:

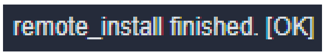
```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

Step 7 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 8 Copy the batch installation commands to the command terminal and press **Enter**.

If the installation package cannot be downloaded, check to ensure the DNS can resolve the domain name in the installation commands.

Step 9 If **remote_install finished. [OK]** is displayed, the installation is successful. Wait for 3 to 5 minutes and check the Docker plug-in status of the panel server.



```
remote_install finished. [OK]
```

----End

13.4 Uninstalling a Plug-in

Uninstall the Docker plug-in if you do not need to use the image blocking function.

Uninstalling a Docker Plug-in

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Installation & Configuration** > **Plug-in Settings**. Click **Plug-In Uninstallation Guide**. In the slide-out panel, copy the commands in the **Uninstallation Commands** section.

Step 4 Remotely log in to the server where the plug-in is to be uninstalled as the **root** user.

- Log in to the ECS console, locate the target server, and click **Remote Login** in the **Operation** column to log in to the server. For details, see Login Using VNC.
- If your server has an EIP bound, you can also use a remote management tool, such as PuTTY or Xshell, to log in to the server and uninstall the plug-in on the server as user **root**.

Step 5 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 6 Create **linux-host-list.txt**, which will contain the server private IP addresses where the plug-in is to be uninstalled:

Command syntax:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
Or echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

To specify multiple IP addresses, write multiple commands, each in a separate line.

Example:

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

Step 7 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 8 Copy the batch uninstallation commands to the command box and press **Enter**. The uninstallation starts automatically.

Step 9 If **remote_uninstall finished. [OK]** is displayed, the uninstallation is successful. Wait for 3 to 5 minutes and check the Docker plug-in status of the panel server.

```
remote_uninstall finished. [OK]
```

----End

14 Authorization

Scenario

Some HSS functions depend on other cloud services. To use these functions, you need to assign HSS the permissions for the cloud service resources.

When you log in to the HSS console, HSS automatically requests the permissions to access other cloud service resources in the current region. After you assign the permissions, HSS will automatically create an agency named **hss_policy_trust** in IAM, which grants HSS the operation permissions on other cloud service resources in your account. For details, see **Cloud Service Delegation**.

To use HSS in multiple regions, request for cloud resource permissions in each region. To view the delegation records of each region, go to the IAM console, choose **Agencies**, and click **hss_policy_trust**.

Table 14-1 describes the cloud service resource permissions that HSS needs you to assign.

Table 14-1 Required permissions on other cloud service resources

Function	Required Permission	Cloud Service Permission		Usage
		Permission	Action	
Container audit (image repository audit)	CTSOperatePolicy	Query audit events	cts:trace:list	Obtain image operation logs (CTS logs of SWR).

Function	Required Permission	Cloud Service Permission		Usage
		Permission	Action	
Installation and configuration on servers	VPCOperatePolicy	Create a port	vpc:ports:create	Create network interface cards (NICs) and modify security groups to ensure that the port used for installing the agent is accessible.
		Delete a port	vpc:ports:delete	
		Create a security group rule	vpc:securityGroupRules:create	
		Delete a security group rule	vpc:securityGroupRules:delete	
		Query the port list or the details about a port	vpc:ports:get	
		Query the network list or the details about a network	vpc:networks:get	
		Query the subnet list or the details about a subnet	vpc:subnets:get	
	VPCEPOperatePolicy	Create an endpoint	vpcep:endpoints:create	Maintain the network channel between the agent and the HSS cloud protection center (master).
		Query the endpoint list	vpcep:endpoints:list	
		Delete an endpoint	vpcep:endpoints:delete	

Function	Required Permission	Cloud Service Permission		Usage
		Permission	Action	
- Installation and configuration on containers - Scheduled repository image synchronization	CCEOperatePolicy	Query cluster information	cce:cluster:get	Manage the lifecycle of HSS-Daemonset and Configmap in a CCE cluster.
		Query clusters in a project	cce:cluster:list	
		Query agencies based on specified conditions	iam:agencies:listAgencies	
Scheduled repository image synchronization	SWROperatePolicy	Query the organization list	swr:namespace:listNamespaces	Obtain information about a specified SWR image repository, including its organization, repository, and artifacts.
		Query the image list	swr:repo:listRepos	
		Query the image tag list	swr:repo:listRepoTags	
		Query the shared image list	swr:repo:listSharedRepos	
		Obtain the instance list	swr:instance:list	
		Obtain details about a synchronized repository	swr:instance:getRegistry	
		Obtain details about a repository	swr:repository:getRepository	
		Obtaining instance details	swr:instance:get	
		Obtain the repository list	swr:repository:listRepositories	
		Obtain the artifact list	swr:repository:listArtifacts	

Prerequisites

To let an IAM user perform operations, assign the **Security Administrator** system role or the **HSS AgencyOperatePolicy** system policy to the user. For details, see **Creating a User Group and Granting Permissions**.

Assigning Cloud Service Resource Permissions

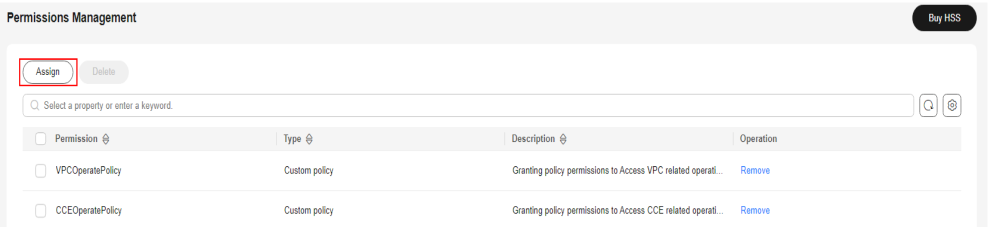
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane, choose **Installation & Configuration** > **Permissions Management**.

Step 4 Click **Assign**. The **Assign** dialog box is displayed.

Figure 14-1 Assigning permissions



Permissions Management

Permission	Type	Description	Operation
VPCOperatePolicy	Custom policy	Granting policy permissions to Access VPC related operati...	Remove
CCEOperatePolicy	Custom policy	Granting policy permissions to Access CCE related operati...	Remove

Step 5 Select permissions and click **OK**.

NOTE

The **Container Audit**, **Server Install & Config**, and **Container Install & Config** pages cannot work properly if required permissions are not assigned. You can click **Assign** in the reminder on the top of the pages to assign permissions.

----End

Deleting Cloud Service Resource Permissions

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

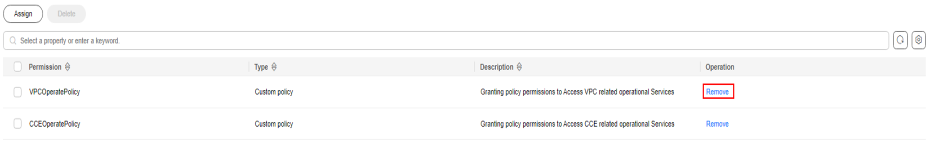
Step 2 In the upper left corner of the page, select a region, click ☰, and choose **Security & Compliance** > **Host Security Service**.

Step 3 In the navigation pane, choose **Installation & Configuration** > **Permissions Management**.

Step 4 Locate a permission and click **Remove** in the **Operation** column. The **Remove Permissions** dialog box is displayed.

Alternatively, select multiple permissions and click **Remove** above the list.

Figure 14-2 Removing permissions



Permission	Type	Description	Operation
VPCOperatePolicy	Custom policy	Granting policy permissions to Access VPC related operational Services	Remove
CCEOperatePolicy	Custom policy	Granting policy permissions to Access CCE related operational Services	Remove

Step 5 Confirm the permission information, enter **DELETE** in the dialog box, and click **OK**.

If the permission is no longer displayed in the permission list, it indicates the permission has been removed.

----End

15 Monitoring and Auditing

15.1 Cloud Eye Monitoring

15.1.1 HSS Monitoring Metrics

Feature Description

This section describes the HSS namespaces, function metrics, and dimensions reported to Cloud Eye. You can view HSS function metrics and alarms by using the Cloud Eye console or calling APIs.

Namespace

SYS.HSS

Metrics

Table 15-1 HSS monitoring metrics

ID	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Original Metric)
host_num	Total Servers	Total number of servers	≥0	Count	N/A	Enterprise Project	300s
unprotected_host_num	Unprotected Servers	Servers for which protection is not enabled	≥0	Count	N/A	Enterprise Project	300s

ID	Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Original Metric)
risky_host_num	Unsafe Servers	Number of servers where risks are detected	≥0	Count	N/A	Enterprise Project	300s
uninstalled_or_offline_agent_num	Servers Without Agent Running	Number of servers where no agent is installed or the agent is offline	≥0	Count	N/A	Enterprise Project	300s
protect_status	Server Protection Status	Whether protection is enabled for a server.	0 or 1 (0: enabled; 1: disabled)	N/A	N/A	Server dimension	300s
agent_status	Agent Running Status	Whether the agent is online	0 or 1 (0: online; 1: offline)	N/A	N/A	Server dimension	300s

Dimensions

Table 15-2 Dimension list

key	Value
hss_enterprise_project_id	Enterprise project ID.
host_id	Server dimension. The value is the server ID.

15.1.2 Configuring a Monitoring Alarm Rule

You can set HSS alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring period, and whether to send notifications. This helps you learn the HSS protection status in a timely manner.

Configuring a Monitoring Alarm Rule

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 On the displayed page, set the parameters as prompted.

For more information, see Creating an Alarm Rule. The key parameters are as follows:

- **Name**: Alarm rule name. The system generates a name, which you can modify.
- **Cloud product**: Select **Host Security Service - Host Security** or **Host Security Service - Server**. **Host Security Service - Host Security** indicates metrics measured by enterprise project, and **Host Security Service - Server** indicates metrics measured by server.
- **Monitoring Scope**: Scope of resources that the alarm rule applies to. You can select **All resources** or **Specific resources**.
- **Method**: Select **Associate template** or **Configure manually**.

NOTE

After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.

Step 7 Configure the alarm notification.

To send alarm notifications via email, SMS, HTTP, or HTTPS, toggle on **Alarm Notification** ( ).

For more information, see Creating an Alarm Rule. The key parameters are as follows:

Step 8 Click **Create**.

----End

15.1.3 Viewing Monitoring Metrics

Cloud Eye can monitor the servers protected by HSS. You can view HSS monitoring metrics on the management console.

Viewing Monitoring Metrics

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

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring**.

Step 5 In the **Dashboard** column, click **Host Security Service HSS**.

Step 6 Select the **Host Security** or **Server** dimension.

Step 7 View monitoring metrics by dimension.

- Host Security

  In the **Operation** column of an enterprise project name, click **View Metric** to view the server protection metric details of the project.

- Server

  In the row of a server, click **View Metric** in the **Operation** column.

----End

15.2 CTS Auditing

15.2.1 HSS Operations Supported by CTS

Cloud Trace Service (CTS) records all operations on HSS, including requests initiated from the management console or open APIs and responses to the requests, for tenants to query, audit, and trace.

Table 15-3 provides more details.

Table 15-3 HSS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Adding or deleting resource tags in batches	hss	changeTmsResourceTagInfo
Provisioning a resource in a scenario	hss	moOpenResourceInfo
Placing an order in a scenario	hss	dealMoOrderInfo
Provisioning a resource	hss	openResourceInfo

Operation	Resource Type	Trace Name
Querying a resource instance	hss	listTmsResourceInstancesInfo
Deleting AOS	hss	deleteAosResourceInfo
Opening AOS resource information	hss	openAosResourceInfo
Deleting tenant information	hss	deleteProjectInfo
Checking whether the licenses exceed the threshold	hss	licenseCheck
Updating a license file	hss	updateLicenseFile
Uploading a license file	hss	uploadLicenseFile
Renewal	hss	dealChargeInfo
Obtaining resource information	hss	getCbcServiceResourceInstances
Changing resource status	hss	changeResourceStatusInfo
Changing a resource	hss	changeResourceInfo
Adding a tag to a resource	hss	addResourceInstanceTag
Deleting a resource tag	hss	deleteResourceInstanceTag
Creating tags in batches	hss	batchCreateTags
Deleting tags in batches	hss	batchDeleteTags
Filtering the number of purchased resources by tag	hss	countResourceInstances
Filtering purchased resources by tag	hss	filterResourceInstanceList
Deleting an authorization policy	hss	deleteIamAgenciesRoles
Binding an authorization policy	hss	createIamAgenciesRoles

Operation	Resource Type	Trace Name
Changing the status of the pay-per-use billing switch for virus scan	hss	changeAntivirusPayPerScanStatus
Changing the number of free virus scans	hss	changeAntivirusFreeQuota
Changing the display status of the pay-per-use billing switch for virus scan	hss	changeAntivirusNotificationStatus
Creating a paid virus scan task	hss	createAntiVirusPaidTask
Creating a custom scan policy	hss	createAntiVirusPolicy
Editing a custom scan policy	hss	changeAntivirusPolicy
Deleting a custom scan policy	hss	deleteAntivirusPolicy
Exporting the virus scan result list	hss	exportAntiVirusResult
Handling virus scan results	hss	operateAntiVirusResult
Creating a virus scan task	hss	createAntiVirusTask
Canceling a scan task	hss	switchAntivirusTask
Deleting a server from the whitelist policy	hss	deleteAppWhitelistPolicyHost
Adding a server to the whitelist policy	hss	addAppWhitelistPolicyHost
Managing the whitelist policy learning status	hss	switchAppWhitelistPolicyLearnStatus
Adding a process to the process whitelist policy	hss	addAppWhitelistPolicyProcess
Marking a process whitelist policy to identify a process	hss	changeAppWhitelistPolicyProcessStatus

Operation	Resource Type	Trace Name
Applying a whitelist policy	hss	switchAppWhitelistPolicyHost
Deleting a whitelist policy	hss	deleteAppWhitelistPolicy
Creating a whitelist policy	hss	createAppWhitelistPolicy
Modifying a whitelist policy	hss	changeAppWhitelistPolicy
Immediately collecting asset fingerprints on a single server	hss	runHostAssetManualCollect1
Changing the port status	hss	batchModifyPortStatus
Exporting container asset fingerprints	hss	downloadAssetFile
Immediately collecting asset fingerprints on a single server	hss	runHostAssetManualCollect
Asset management - server management - configuring asset importance	hss	addValuesLevel
Modifying the backup policy associated with the vault	hss	updateBackupPolicyInfo
Ignoring, unignoring, repairing, or verifying the failed configuration check items	hss	changeCheckRuleAction
Ignoring, unignoring, repairing, or verifying the failed configuration check items that failed to pass the check	hss	changeCheckRuleAction
Deleting a specified configuration check policy	hss	deleteSecurityCheckPolicyGroup

Operation	Resource Type	Trace Name
Modifying information about a specified configuration check policy	hss	updateSecurityCheckPolicyGroup
Creating a configuration check policy	hss	addSecurityCheckPolicyGroup
Unbinding quota	hss	cancelHostsQuota
Querying quota IDs in batches	hss	listResourceIds
Exporting the container cluster protection event list	hss	exportClusterProtectEventInfo
Changing the alarm status	hss	modClusterEvents
Deleting a cluster protection policy	hss	deleteClusterProtectionPolicy
Creating a cluster protection policy	hss	createClusterProtectionPolicy
Modifying a cluster protection policy	hss	changeClusterProtectionPolicy
Managing the cluster protection mode	hss	switchClusterProtectionMode
Creating a container export task	hss	exportContainerList
Deleting a cluster daemonset	hss	deleteAgentDaemonset
Creating a cluster daemonset	hss	createAgentDaemonset
Updating a cluster daemonset	hss	updateAgentDaemonset
Obtaining cluster configurations	hss	getCCEClusterConfig
Uninstalling daemonsets in batches	hss	batchDeleteAgentDaemonset

Operation	Resource Type	Trace Name
Upgrading cluster daemonsets in batches	hss	batchUpgradeAgentDaemonset
Obtaining cluster node tags	hss	listCCENodesLabel
Enabling protection for a cluster	hss	addCceIntegrationProtection
Obtaining container cluster risk information in batches	hss	getCCEClusterDetectRiskList
Creating a multi-cloud cluster	hss	createMultiCloudClusters
Deleting a multi-cloud cluster	hss	removeMultiCloudClusters
Updating a multi-cloud cluster	hss	updateMultiCloudClusters
Synchronizing the access status of a multi-cloud cluster	hss	syncMultiCloudClusterStatus
Parsing the configuration file of a multi-cloud cluster	hss	parseMultiCloudClusterConfig
Changing protection status	hss	switchContainerProtectStatus
Creating a security group policy	hss	createSecurityGroupPolicy
Updating a security group policy	hss	updateSecurityGroupPolicy
Deleting a configuration policy of the container cluster network	hss	deleteContainerNetworkPolicy
Adding a configuration policy to the container cluster network	hss	createContainerNetworkPolicy
Updating a configuration policy of the container cluster network	hss	updateContainerNetworkPolicy

Operation	Resource Type	Trace Name
Deleting a security group policy	hss	deleteSecurityGroupPolicy
Exporting emergency malicious programs	hss	exportEmergency
Handling incidents	hss	handleMalwareEvent
Managing the isolation switch	hss	isolateOperateEmergency
Restoring an isolated file	hss	recoverIsolateFile
Handling alarms in batches	hss	batchChangeEvent
Unblocking an IP address	hss	changeBlockedIp
Exporting vulnerabilities	hss	exportEventRequest
Deleting an isolated file	hss	deleteIsolatedFile
Restoring an isolated file	hss	changeIsolatedFile
Handling an alarm event	hss	changeEvent
Removing an alarm from whitelist	hss	removeAlarmWhiteList
Importing an alarm whitelist	hss	importAlarmWhiteList
Removing login information from login whitelist	hss	removeLoginWhiteList
Configuring the login whitelist	hss	addLoginWhiteList
Removing an item from the system user whitelist	hss	removeSystemUserWhiteList
Adding an item to the system user whitelist	hss	addSystemUserWhiteList
Modifying the system user whitelist	hss	updateSystemUserWhiteList

Operation	Resource Type	Trace Name
Exporting a task	hss	exportTaskInfo
Enabling protection for new servers by default	hss	switchDecoyPortAutoBind
Disabling HSS	hss	deleteDecoyPortHostPolicy
Changing the server protection policy	hss	switchDecoyPortHostPolicy
Creating a protection policy	hss	createDecoyPortPolicy
Deleting a server protection policy	hss	deleteDecoyPortPolicy
Editing a protection policy	hss	modifyDecoyPortPolicy
Enabling or disabling a protection policy	hss	switchDecoyPortPolicy
Ignoring or unignoring a server	hss	changeHostIgnoreStatus
Delivering a manual scan	hss	setManualDetect
Configuring asset importance	hss	associateHostAssetValue
Modifying the firewall authorization status	hss	switchFirewallStatus
Adding a server to group	hss	associateHostsGroup
Deleting a server group	hss	deleteHostsGroup
Creating a server group	hss	addHostsGroup
Editing a server group	hss	changeHostsGroup
Creating an on-premise data center server group	hss	addOutsideHostGroup
Editing an on-premises data center server group	hss	changeOutsideHostGroup

Operation	Resource Type	Trace Name
Changing protection status	hss	switchHostsProtectStatus
Switching editions	hss	switchHostsProtectVersion
Uninstall an agent	hss	uninstallAgents
Upgrading an agent	hss	upgradeAgents
Creating a VPC endpoint	hss	createVpcEndpoint
Querying the creation status of each server endpoint	hss	showEndpointStatus
Creating a service order	hss	createDealOrder
Changing specifications	hss	upgradeOrder
Batch exporting baseline check results of the SWR image repository	hss	batchExportBaselineTask
Changing the user-defined weak password of an image	hss	changeExtendedWeakPassword
Scanning images in the image repository in batches	hss	batchScanSwrImage
Scanning local images	hss	batchScanLocalImage
Batch exporting local image vulnerabilities	hss	batchExportLocalVulList
Batch exporting local image vulnerabilities	hss	batchExportLocalVulTask
Scanning SWR images in batches	hss	batchScanPrivateImage
Exporting image security report export statistics	hss	showImageSecurityReportStatistic

Operation	Resource Type	Trace Name
Modifying the whitelist of file paths containing sensitive image information	hss	changeFilePathWhiteDetail
Sensitive information processing	hss	changeSensitiveInfo
Updating images shared by others from SWR	hss	sharedImageSynchronization
Batch exporting SWR image repository vulnerabilities	hss	batchExportSWRVulList
Updating and scanning an SWR image	hss	runSwrImageScan
Batch exporting SWR image repository vulnerabilities	hss	batchExportSWRVulTask
Synchronizing the image list from SWR	hss	runImageSynchronize
Synchronizing private and shared images from SWR	hss	runImageSynchronizeTask
Scanning images	hss	runImageScan
(Operation tool) Clearing the search history of the tool	hss	deleteToolConditionHistory
(Operation tool) Using the tool to search	hss	executeTool
Managing the container lifecycle	hss	changeContainerStatus
Synchronizing cluster information	hss	createClustersInfo
Running a cluster script	hss	createDaemonset
Running a cluster script	hss	createDaemonset

Operation	Resource Type	Trace Name
Changing the status of the monthly operations report dialog box	hss	changeMonthlyOperationReport-TipStatus
Performing a security check again	hss	resetRiskScore
Modifying a policy	hss	changePolicyDetail
Applying a policy group	hss	associatePolicyGroup
Removing a policy group	hss	deletePolicyGroup
Modifying a policy group	hss	changePolicyGroup
Copying a server policy group	hss	addPolicyGroup
Deleting a server from the whitelist policy	hss	deletePWLPolicyHost
Applying a whitelist policy	hss	switchPWLPolicyHost
Adding a server to the whitelist policy	hss	addPWLPolicyHost
Marking a process whitelist policy to identify a process	hss	changePWLPolicyProcessStatus
Re-learning a whitelist policy	hss	relearnPWLPolicy
Handling an event	hss	operatePWLEvent
Deleting a whitelist policy	hss	deletePWLPolicy
Modifying a whitelist policy	hss	changePWLPolicy
Creating a whitelist policy	hss	createPWLPolicy
Creating a quota order	hss	createQuotasOrder
Applying a backup policy to a vault	hss	associateBackupPolicy

Operation	Resource Type	Trace Name
Enabling backup for a single server	hss	startBackupSingle
Enabling backup for a single server	hss	startSingleBackup
Deleting a backup	hss	deleteDuplicationInfo
Restoring data from a backup	hss	restoreDuplicationInfo
Ignoring a prompt	hss	updateAutoDeployAgent
Enabling ransomware prevention	hss	batchStartProtection
Disabling ransomware prevention	hss	stopProtection
Enabling ransomware prevention	hss	startProtection
Enabling ransomware protection for a single server	hss	startProtectionSingle
Deleting a policy	hss	deleteProtectionPolicy
Adding a protection policy	hss	addProtectionPolicy
Modifying a ransomware protection policy	hss	updateProtectionPolicy
Switching a ransomware protection policy	hss	associateProtectionPolicy
Deleting a protection policy	hss	deletePolicy
Adding a protection policy	hss	addPolicy
Modifying a policy	hss	updatePolicy
Enabling/Disabling application protection	hss	switchRasp
Uploading a security report logo	hss	uploadReportLogo

Operation	Resource Type	Trace Name
Changing the security report switch	hss	switchReportStatus
Deleting a report	hss	deleteSecurityReport
Creating or copying a report	hss	addSecurityReport
Modifying a report	hss	changeSecurityReport
Sending a report	hss	sendSecurityReport
Modifying the scheduled configuration of a security check	hss	updateSecurityCheckConfig
Manually starting a health check	hss	startManualSecurityCheck
Canceling a manually started health check	hss	stopManualSecurityCheck
Deleting a user-built cluster daemonset	hss	deleteSelfBuiltClusterDaemonset
Saving a user-built cluster daemonset	hss	saveSelfBuiltClusterDaemonset
Installing the agent	hss	installAgent
Configuring alarms	hss	updateAlarmConfig
Installing agents in batches	hss	batchInstallAgent
Enabling or disabling the automatic agent upgrade function	hss	changeAgentAutoUpgradeStatus
Enabling or disabling the automatic quota binding function	hss	changeAutoOpenQuotaStatus
Adding, editing, or deleting common login IP addresses	hss	modifyLoginCommonIp
Adding, editing, or deleting common login locations	hss	modifyLoginCommonLocation
Adding, editing, or deleting a login IP address whitelist	hss	modifyLoginWhiteIp

Operation	Resource Type	Trace Name
Enabling or disabling malware sample collection for cloud scan	hss	changeMalwareCollectStatus
Setting prompt information	hss	setMalwareReminders
Setting prompt information	hss	setRemindersConfig
Uploading a template file	hss	uploadTemplate
Configuring two-factor login	hss	setTwoFactorLoginConfig
Enabling or disabling automatic isolation and killing of malicious programs	hss	changeAutoKillVirusStatus
Upgrading from agent 1.0 to agent 2.0	hss	upgradeAgent
Restarting a server where vulnerabilities were fixed	hss	changeVulRestart
Exporting emergency vulnerabilities	hss	exportEmergencyVulnerabilities
Operating emergency vulnerabilities	hss	emergencyOperate
Exporting information about vulnerabilities and affected servers	hss	exportVuls
Scanning for vulnerabilities	hss	createVulnerabilityScanTask
Ignoring or unignoring the servers affected by the selected software vulnerability	hss	changeVulStatus1
Performing rollback using a backup	hss	restoreVulHostBackup

Operation	Resource Type	Trace Name
Querying the backup statistics of the servers where vulnerabilities were handled	hss	showVulBackupStatistics
Creating a task for exporting historical vulnerabilities	hss	exportHandledVulnerabilities
Querying the vulnerability fixing command list	hss	listVulRepairCmds
Vulnerability management - server view - server list - displaying report	hss	showVulReportData
Vulnerability management - server view - server list - exporting report	hss	exportVulReport
Modifying a vulnerability scan policy	hss	changeVulScanPolicy
Rescanning servers in the previous vulnerability scan job	hss	rescanVulScanTask
Querying the estimated time of vulnerability scan tasks	hss	showVulScanTaskEstimatedTime
Modifying a vulnerability scan policy	hss	changeVulScanPolicy
Creating a scan task	hss	createVulnerabilityScanTask
Changing the status of a vulnerability	hss	changeVulStatus
Recording the last time when a user viewed the vulnerability task management page	hss	recordUserViewVulTask

Operation	Resource Type	Trace Name
Removing a vulnerability whitelist item	hss	deleteVulWhiteList
Adding a vulnerability whitelist item	hss	addVulWhiteList
Modifying the vulnerability whitelist	hss	changeVulWhiteList
Enabling or disabling dynamic WTP	hss	setRaspSwitch
Setting the trustworthy status of a privileged process and its subprocesses	hss	setPrivilegedChildStatus
Enabling or disabling WTP	hss	setWtpProtectionStatusInfo
Setting the period for automatically disabling protection	hss	setDateOffConfigInfo
Setting the status of the monitoring-only switch	hss	setMonitorOnlyStatus
Removing a privileged process	hss	deletePrivilegedProcessInfo
Adding a privileged process	hss	addPrivilegedProcessInfo
Modifying a privileged process	hss	updatePrivilegedProcessInfo
Removing a protected directory	hss	deleteHostProtectDirInfo
Adding a protected directory	hss	addHostProtectDirInfo
Modifying a protected directory	hss	updateHostProtectDirInfo
Enabling or disabling directory protection	hss	setProtectDirSwitchInfo
Modifying the Tomcat bin directory for dynamic WTP	hss	updateRaspPathInfo

Operation	Resource Type	Trace Name
Enabling or disabling remote backup	hss	setRemoteBackupInfo
Setting the status of scheduled protection	hss	setTimingOffSwitchInfo
Deleting scheduled protection settings	hss	deleteTimingOffConfigInfo
Adding a scheduled protection setting	hss	addTimingOffConfigInfo
Modifying scheduled protection settings	hss	updateTimingOffConfigInfo
Removing a remote backup server	hss	deleteBackupHostInfo
Adding or modifying a remote backup server	hss	updateBackupHostInfo
Querying software information through file upload	hss	showFileAppInfoList
Importing the feature library upgrade package	hss	importFeatureUpload21
Deleting an account	hss	deleteAccount
Adding accounts in batches	hss	batchAddAccounts
Enabling a trusted service	hss	enableTrustService

15.2.2 Viewing CTS Traces in the Trace List

Scenarios

After you enable Cloud Trace Service (CTS) and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, CTS starts recording operations on data in Object Storage Service (OBS) buckets. CTS stores operation records (traces) generated in the last seven days.

This section describes how to query or export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.
- These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

Viewing Real-Time Traces in the Trace List of the New Edition

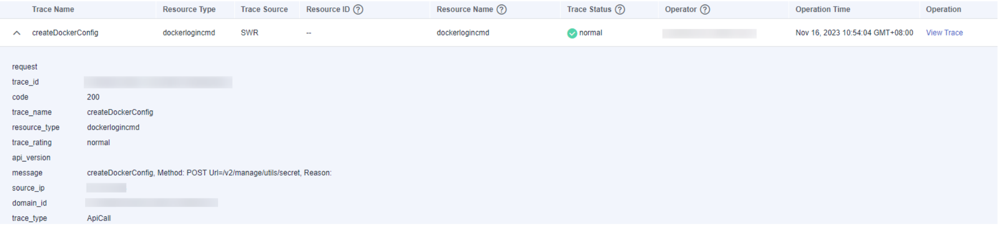
1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
   - **Enterprise Project ID**: Enter an enterprise project ID.
   - **Access Key**: Enter a temporary or permanent access key ID.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.

- Enter any keyword in the search box and press **Enter** to filter desired traces.
- Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
- Click ⟳ to view the latest information about traces.
- Click ⚙ to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (●), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.

6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

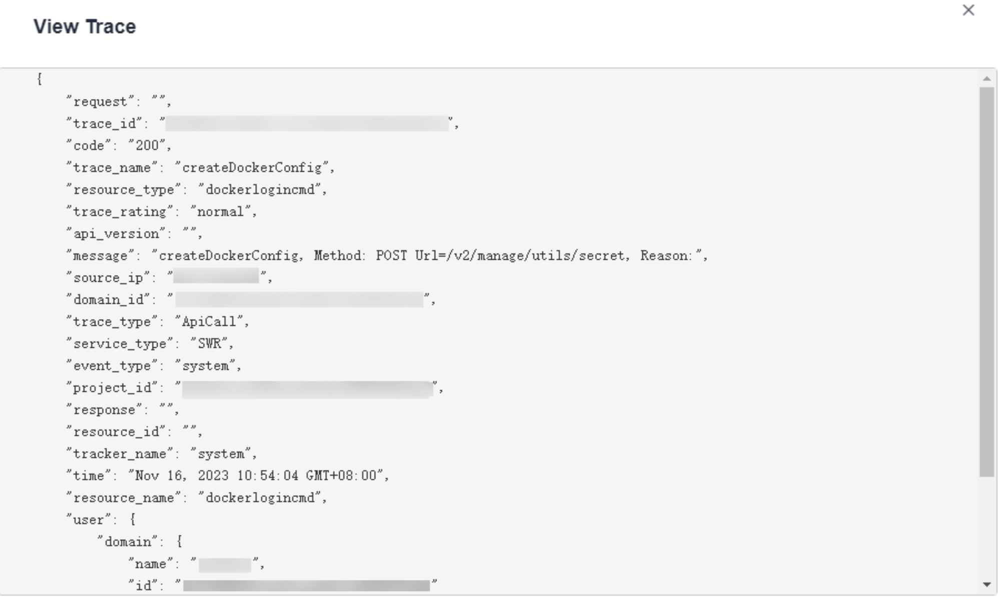
1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available.
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
   - Click ⟳ to view the latest information about traces.
8. Click ⌄ on the left of a trace to expand its details.



	Trace Name	Resource Type	Trace Source	Resource ID ⓘ	Resource Name ⓘ	Trace Status ⓘ	Operator ⓘ	Operation Time	Operation
^	createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	✓ normal	[redacted]	Nov 16, 2023 10:54:04 GMT+08:00	View Trace

request	
trace_id	[redacted]
code	200
trace_name	createDockerConfig
resource_type	dockerlogincmd
trace_rating	normal
api_version	
message	createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:
source_ip	[redacted]
domain_id	[redacted]
trace_type	ApiCall

9. Click **View Trace** in the **Operation** column. The trace details are displayed.



View Trace

```
{
    ”request”: ””,
    ”trace_id”: ”[redacted]”,
    ”code”: ”200”,
    ”trace_name”: ”createDockerConfig”,
    ”resource_type”: ”dockerlogincmd”,
    ”trace_rating”: ”normal”,
    ”api_version”: ””,
    ”message”: ”createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:”,
    ”source_ip”: ”[redacted]”,
    ”domain_id”: ”[redacted]”,
    ”trace_type”: ”ApiCall”,
    ”service_type”: ”SWR”,
    ”event_type”: ”system”,
    ”project_id”: ”[redacted]”,
    ”response”: ””,
    ”resource_id”: ””,
    ”tracker_name”: ”system”,
    ”time”: ”Nov 16, 2023 10:54:04 GMT+08:00”,
    ”resource_name”: ”dockerlogincmd”,
    ”user”: {
        ”domain”: {
            ”name”: ”[redacted]”,
            ”id”: ”[redacted]”
```

10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

16 Enterprise Project Management

16.1 Managing Projects and Enterprise Projects

Selections are available only if you have enabled the enterprise project function, or your account is an enterprise account. To enable this function, contact your customer manager. An enterprise project provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.

Creating a Project and Assigning Permissions

- Creating a project

  Log in to the management console, click the username in the upper right corner, and select **Identity and Access Management**. In the navigation pane on the left, choose **Projects**. In the right pane, click **Create Project**. On the displayed **Create Project** page, select a region and enter a project name.

- Granting permissions

  You can assign permissions (of resources and operations) to user groups to associate projects with user groups. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. On the **User Groups** page of the IAM console, locate the target user group and click **Authorize** in the **Operation** column. Grant permissions to the project.

     For details, see **Granting a User Group Permissions for a Project** in the IAM help.

  b. On the **Users** page, click a username to go to the details page. In the **User Groups** area, add a user group for the user.

Creating an Enterprise Project and Assigning Permissions

- Creating an enterprise project

  On the management console, click **Enterprise** in the upper right corner. The **Project Management** page is displayed. In the upper right corner of the **Project Management** page, click **Create Enterprise Project** and create a project as prompted.

NOTE

Enterprise is available on the management console only if you have enabled the enterprise project, or you have an enterprise account. To enable this function, contact customer service.

- Granting permissions

  You can add a user group to an enterprise project and configure a policy to associate the enterprise project with the user group. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. On the **Project Management** page, click the name of an enterprise project to go to its details page.

  b. On the **Permissions** tab, click **Authorize User Group** to go to the **User Groups** page on the IAM console. Associate the enterprise project with a user group and assign permissions to the group.

     For details, see **Creating a User Group and Assigning Permissions** in the IAM help.

- Associating HSS with enterprise projects

  You can use enterprise projects to manage cloud resources.

  – Select an enterprise project when purchasing HSS.

    On the page for buying HSS, select an enterprise project from the **Enterprise Project** drop-down list.

  – Adding resources

    On the **Enterprise Project Management** page, you can add existing ECSs/BMSs to an enterprise project.

    Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.

  For more information, see **Creating an Enterprise Project**.

16.2 Managing All Projects Settings

If you have enabled the enterprise project function, you can select **All projects** from the **Enterprise Project** drop-down list and batch set all servers under all your projects.

- Binding quotas to servers

  Under **All projects**, you can bind the quota of an enterprise project to a server of another project. The project that the quota belongs to will be billed for the quota.

- Batch installation and configuration

  Configure the alarm whitelist, Login Whitelist, malicious program isolation and killing, and alarm notifications for all servers.

- Applying a policy group

  The policy groups under **All projects** can be applied to any servers in any enterprise projects protected by the premium edition.

The policy groups under **All projects** do not belong to any specific projects and do not affect the policy groups under any other projects.

- Subscribing to security reports under **All projects**

  The security reports under **All projects** do not belong to any specific projects and do not affect the security reports under any other projects.

You can configure uniform settings for all projects under **All projects** and customize settings under a specific project. The settings under an enterprise project do not affect those under other enterprise projects.

Prerequisites

You have the **Tenant Administrator** or **HSS Administrator+Tenant Guest** permissions.

Binding Quotas to Servers

Perform the following steps to bind the WTP edition quota to a server under **All projects**.

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

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

Step 3 Choose **Asset Management** > **Servers & Quota** and click **Quotas**. The server protection quotas are displayed.

Step 4 In the quota list, select a quota whose **Usage Status** is **Idle** and click **Bind Server**.

Step 5 Select servers in the **Bind Server** dialog box.

Step 6 Click **OK**. The **Protection Status** of the server will change to **Enabled**.

----End

Binding Quotas to Containers

Perform the following steps to bind the container edition quota to a server under **All projects**.

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

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

Step 3 Choose **Asset Management** > **Containers & Quota** and click **Protection Quotas**. The server protection quotas are displayed.

Step 4 In the quota list, select a quota whose **Usage Status** is **Idle** and click **Bind Server**.

Step 5 Click the **Container Nodes** tab. Locate the target server and click **Enable Protection** in the **Operation** column.

The status of the server to be protected must be **Normal**, and the agent status must be **Online**.

Step 6 Select servers in the **Bind Server** dialog box.

In the displayed dialog box, select **Yearly/Monthly**, read the *Container Guard Service Disclaimer*, and select **I have read and agreed to Container Guard Service Disclaimer**.

The quota can be allocated in the following ways:

- **Select a quota randomly**: Let the system allocate the quota with the longest remaining validity to the server.
- Select a quota ID and allocate it to a server.

Step 7 Click **OK**. The **Protection Status** of the server will change to **Enabled**.

----End