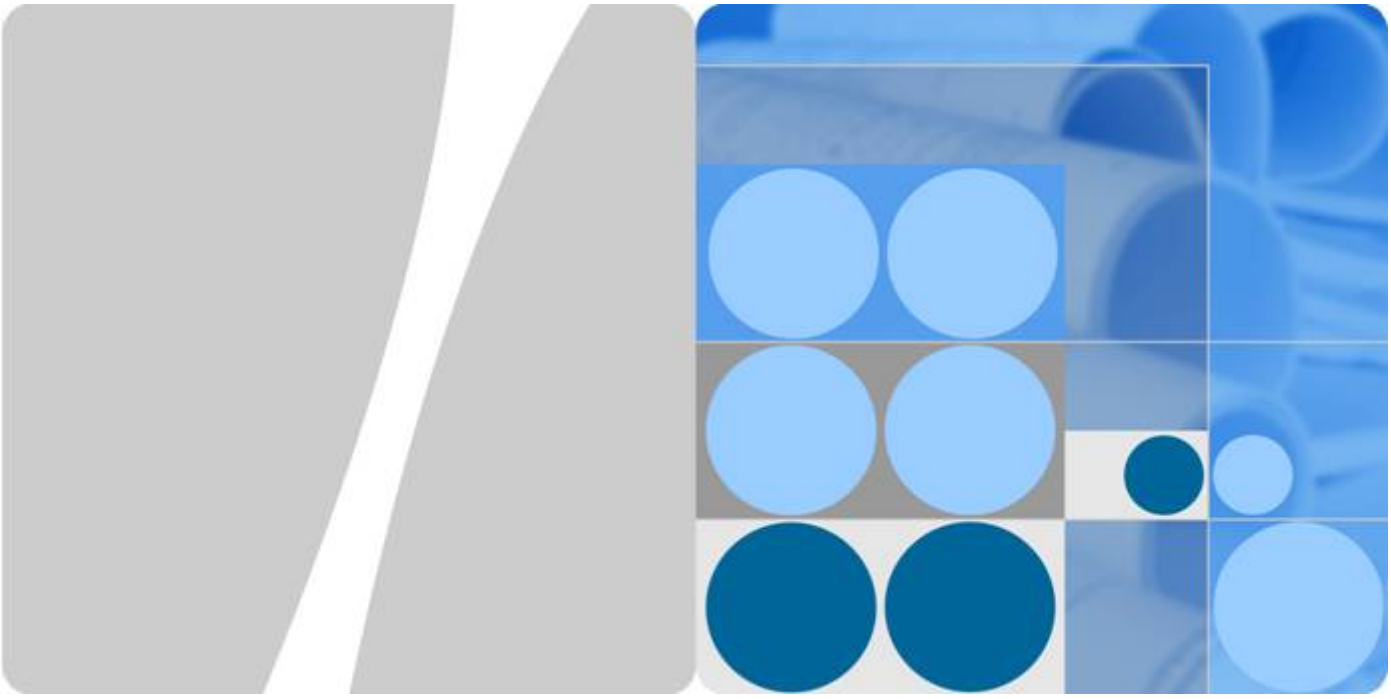


Host Security Service

User Guide

Date **2021-06-30**

Contents

1 Introduction

1.1 HSS

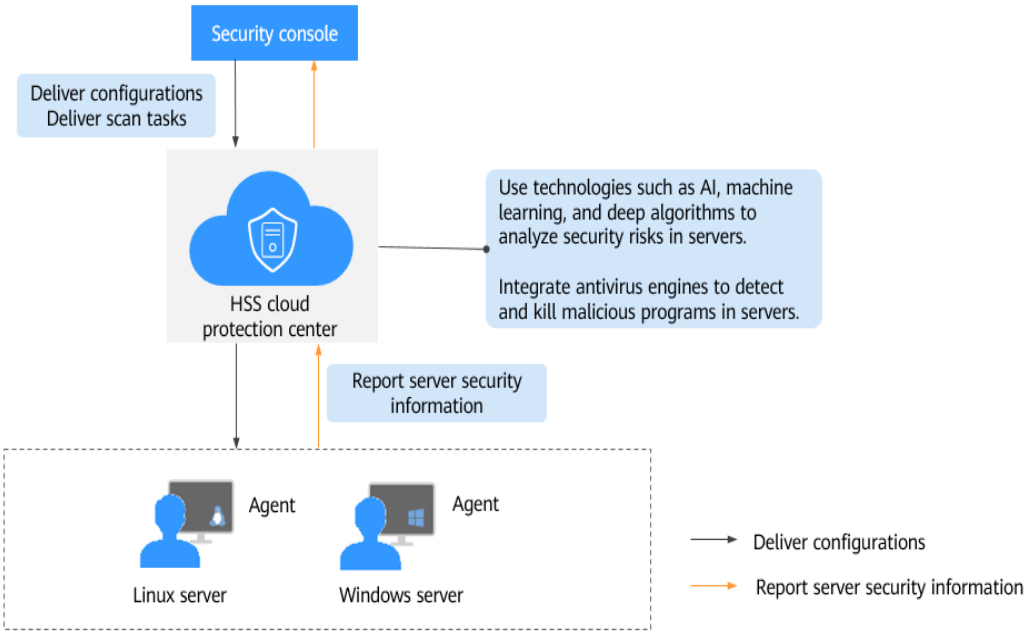
Host Security Service (HSS) helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

Working Principles

Install the HSS agent on your servers, and you will be able to check the server security status and risks in a region on the HSS console.

Figure 1-1 illustrates how HSS works.

Figure 1-1 Working principles



The following table describes HSS components.

Table 1-1 Components

Component	Description
Management console	A visualized management platform, where you can apply configurations in a centralized manner and view the defense status and scan results of servers in a region.
HSS cloud protection center	• Uses technologies such as AI, machine learning, and deep algorithms to analyze security risks in servers. • Integrates multiple antivirus engines to detect and kill malicious programs in servers. • Receives configurations and scan tasks sent from the console and forwards them to agents on the servers. • Receives server information reported by agents, analyzes security risks and exceptions on servers, and displays the analysis results on the console.
Agent	• Communicates with the HSS cloud protection center via HTTPS and WSS. Port 443 is used by default. • Scans all servers every early morning; monitors the security status of servers; and reports the collected server information (including non-compliant configurations, insecure configurations, intrusion traces, software list, port list, and process list) to the cloud protection center. • Blocks server attacks based on the security policies you configured. **NOTE** • If the agent is not installed or is abnormal, HSS is unavailable. • Select the agent and installation command suitable for your OS. • Web Tamper Protection (WTP) and HSS can use the same agent on a server.

1.2 Functions and Features

HSS provides asset management, vulnerability management, intrusion detection, baseline inspection, and web tamper protection (WTP) functions.

Asset Management

Deeply scan the accounts, ports, processes, web directories, software information, and auto-started tasks on your servers. You can manage all your information assets on the **Assets** page.

Table 1-2 Asset management

Function	Description	Check Mode
Account information management	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 **Account ID**, server quantity and names, **Administrator Rights**, **User Group**, **User Directory**, and **User Startup Shell**. • The operation history of an account includes the **Action**, **Account ID**, **Administrator Rights**, **User Group**, **User Directory**, **User Startup Shell**, and **Time** of the action.	Real-time check
Open port check	Check open ports on your servers, including risky and unknown ports. You can check **Port Type**, **Servers**, **Risk Level**, **Status**, **Port Description**, and the specific **Server**, **Bound IP Address**, **Status**, **PID**, and **Program File** of a port.	Real-time check
Process check	Check processes on your servers and find abnormal processes. You can check **Process Name**, **Servers**, **Total Number of Processes**, **Total Number of File Names**, and the specific **Server**, **Process Path**, **File Permission**, **User**, **PID**, and startup time of a process.	Real-time check
Web directory management	Check and manage directories used by web services on your servers. You can check the **File Path**, **Application Type**, **Local Port**, **URL**, **PID**, and **Program File**.	Real-time check
Software information management	Check and manage all software installed on your servers, 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**, server quantity and names, and **Software Version**. • The software operation history includes **Action**, **Software Name**, **Software Version**, and **Time**. • You can use the manual detection function to check software information.	• Automatic check in the early morning every day • Manual check

Function	Description	Check Mode
Auto-startup	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.	Real-time check

Vulnerability Management

The vulnerability management function detects vulnerabilities and risks in Linux OSs, Windows OSs, and Web content management systems (Web-CMSs).

Table 1-3 Vulnerability management

Function	Description	Check Mode
Software vulnerability detection	Check vulnerabilities in Linux and Windows OSs. Check and handle vulnerabilities in your system and the software (such as SSH, OpenSSL, Apache, and MySQL) you obtained from official sources and have not compiled.	• Automatic check in the early morning every day • Manual check
Web-CMS vulnerability detection	Check and handle vulnerabilities found by scanning web directories and files in your Web-CMS.	

Baseline Inspection

The baseline check function detects risky configurations of server systems and key software.

Table 1-4 Baseline inspection

Function	Description	Check Mode
Password policy check	• Check whether your password complexity policy is proper and modify it based on suggestions provided by HSS, improving password security. • You can use the manual detection function to check password complexity policies.	• Automatic check in the early morning every day • Manual check
Common weak password detection	• Check for weak passwords and remind users to change them, preventing easy guessing. • On the **Common Weak Password Detection** tab, you can view the account name, account type, and usage duration of a weak password. • You can use the manual detection function to detect weak passwords on servers.	• Automatic check in the early morning every day • Manual check
Unsafe configuration item check	Check for unsafe Tomcat, Nginx, and SSH login configurations. On the **Configure Detection** page, you can view the description, matched detection rule, threat level, and status of a configuration. • You can handle risky configuration items and ignore trusted items based on the detection rules and detection results. • You can use the manual detection function to check key configurations.	• Automatic check in the early morning every day • Manual check

Intrusion Detection

The intrusion detection function identifies and prevents intrusion to servers, discovers risks in real time, detects and kills malicious programs, and identifies web shells and other threats.

Table 1-5 Intrusion detection

Intrusion	How HSS Detects It	Check Mode
Brute-force attack	Detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts. ● If the number of brute-force attacks from an IP address reaches 5 within 30 seconds, the IP address will be blocked. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. ● You can check whether the 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.	Real-time check
Abnormal login	Detect abnormal login behavior, such as remote login and brute-force attacks. ● Check and handle remote logins. HSS can check the blocked login IP addresses, and who used them to log in to which servers at what time. If a user's login location is not any common login location you set, an alarm will be triggered. ● Trigger an alarm if a user logs in by a brute-force attack.	Real-time check
Malicious program (cloud scan)	Check and kill malware, such as viruses, Trojan horses, web shells, worms, mining software, unknown malicious programs, and variants. All this can be done with just a few clicks. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing. You can manually isolate and kill identified and suspicious malicious programs, and cancel the isolation of and ignore trusted programs.	Real-time check
Abnormal process behavior	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. The following abnormal process behavior can be detected: ● Abnormal CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections	Real-time check

Intrusion	How HSS Detects It	Check Mode
Changes made to critical files	• Check alarms about modifications on key files (such as **ls**, **ps**, **login**, and **top**). • Key file change information includes the paths of modified files, the last modification time, and names of the servers storing configuration files.	Real-time check
Web shells	Check whether the files (often PHP and JSP files) 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.	• Real-time check • Manual check
Reverse shell	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.	Real-time check
Abnormal shell	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	Real-time check
High-risk command execution	Check executed commands in real time and generate alarms on high-risk commands.	Real-time check
Auto-startup check	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders.	Real-time check
Unsafe account	Scan accounts on servers and list suspicious accounts in a timely manner. You can check the name, user group, UID/SID, user directory, and startup shell of an account.	Real-time check
Privilege escalation	Detect privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities • File privilege escalation	Real-time check

Intrusion	How HSS Detects It	Check Mode
Rootkit	Detect suspicious rootkit installation in a timely manner by checking: • File signatures • Hidden files, ports, processes, and kernel modules	Automatic check every day

Advanced Protection

Function	Description	Check Mode
Application recognition service (ARS)	Set whitelist policies, and determine whether applications are **Trusted**, **Untrusted**, or **Unknown**. The applications that are not whitelisted are not allowed to run. This function protects your servers from untrusted or malicious applications, reducing unnecessary resource usage.	Real-time check
File integrity monitoring (FIM)	Check the files in the Linux OS, applications, and other components to detect tampering.	Real-time check
Ransomware prevention	Analyze operations on servers, identify trusted applications, and report alarms on or block untrusted applications, depending on your settings.	Real-time check

WTP

Web Tamper Protection (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.

Table 1-6 WTP

Function	Description	Check Mode
Static WTP	Prevents static web page files on website servers from being tampered with.	Real-time check
Net disk tampering prevention	Prevents web page files in shared net disks from being tampered with.	

Function	Description	Check Mode
Dynamic WTP	Prevents dynamic web page content in website databases from being tampered with.	

1.3 Advantages

HSS helps you manage and maintain the security of all your servers and reduce common risks.

Centralized Management

You can check for and fix a range of security issues on a single console, easily managing your servers.

- On the security console, you can view the sources of server risks in a region, handle them according to displayed suggestions, and use filter, search, and batch processing functions to quickly analyze the risks of all servers in the region.

Accurate Defense

HSS blocks attacks with pinpoint accuracy by using advanced detection technologies and diverse libraries.

All-Round Protection

HSS protects servers against intrusions by prevention, defense, and post-intrusion scan.

Lightweight Agent

The agent occupies only a few resources, not affecting server system performance.

1.4 Editions

HSS provides basic, enterprise, premium, and WTP editions. **Table 1-7** describes their functions. For more details, see **Functions and Features**.

Table 1-7 Edition details

Function	Item	Description	Basic	Enterprise	Premium	WTP
Asset Management	Manage account information	Check and manage server accounts all in one place.	×	√	√	√
	Check open ports	Check open ports all in one place and identify high-risk and unknown ports.	×	√	√	√
	Manage applications	Check running applications all in one place and identify malicious applications.	×	√	√	√
	Web directory management	Check and manage web directories all in one place.	×	√	√	√
	Manage software	Check and manage server software all in one place and identify insecure versions.	×	√	√	√
	Manage auto-startup	Check auto-startup entries and collect statistics on entry changes in a timely manner.	×	×	√	√
Vulnerability management	Windows vulnerabilities	Scan Windows OS and software for vulnerabilities based on vulnerability databases, receive alarms generated on critical vulnerabilities, and manage them all in one place.	×	√	√	√
	Linux vulnerabilities	Scan Linux OS and software for vulnerabilities based on vulnerability databases, receive alarms generated on critical vulnerabilities, and manage them all in one place.	×	√	√	√

Function	Item	Description	Basic	Enterprise	Premium	WTP
	Web-CMS vulnerabilities	Check and handle Web-CMS vulnerabilities found in web directory and file scans.	×	√	√	√
Unsafe settings check	Password policy check	Check password complexity policies and modify them based on suggestions provided by HSS to improve password security.	√	√	√	√
	Weak password check	Change weak passwords to stronger ones based on HSS scan results and suggestions.	√	√	√	√
	Unsafe configuration item check	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.	×	√	√	√
Intrusion detection	Brute-force attack	Your accounts are protected from brute-force attacks. HSS will block the attacking hosts when detecting such attacks.	√	√	√	√

Function	Item	Description	Basic	Enterprise	Premium	WTP
	Abnormal login	Detect abnormal login behavior, such as remote login and brute-force attacks. • Check and handle remote logins. HSS can check the blocked login IP addresses, and who used them to log in to which servers at what time. If a user's login location is not any common login location you set, an alarm will be triggered. • Trigger an alarm if a user logs in by a brute-force attack.	√	√	√	√
	Malicious program (cloud scan)	Check and handle detected malicious programs all in one place, including web shells, Trojan horses, mining software, worms, and viruses.	×	√	√	√

Function	Item	Description	Basic	Enterprise	Premium	WTP
	Abnormal process behavior	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 CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections	×	√	√	√
	Change in critical file	Receive alarms when critical system files are modified.	×	√	√	√
	Web shell	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 scan for web shells on servers.	×	√	√	√

Function	Item	Description	Basic	Enterprise	Premium	WTP
	Reverse shell	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.	×	×	√	√
	Abnormal shell	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	×	×	√	√
	High-risk command execution	Receive real-time alarms on high-risk commands.	×	×	√	√
	Auto-startup check	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders.	×	×	√	√
	Unsafe account	Scan accounts on servers and list suspicious accounts in a timely manner.	×	√	√	√

Function	Item	Description	Basic	Enterprise	Premium	WTP
	Privilege escalation	Detect privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities ● File privilege escalation	×	×	√	√
	Rootkit	Detect suspicious rootkit installation in a timely manner by checking: ● Check rootkits based on file signatures. ● Hidden files, ports, processes, and kernel modules	×	×	√	√
Advanced protection	Program management	Set whitelist policies, and determine whether applications are **Trusted**, **Untrusted**, or **Unknown**. The applications that are not whitelisted are not allowed to run. This function protects your servers from untrusted or malicious applications, reducing unnecessary resource usage.	×	×	√	√
	Monitor file integrity	Check the files in the Linux OS, applications, and other components to detect tampering.	×	×	√	√

Function	Item	Description	Basic	Enterprise	Premium	WTP
	Ransomware prevention	Analyze operations on servers, identify trusted applications, and report alarms on or block untrusted applications, depending on your settings.	×	×	√	√
Security operations	Policy management	You can define and issue different detection policies for different servers or server groups, implementing refined security operation. ● View the policy list. ● Create a policy group based on default and existing policy groups. ● Define a policy. ● Edit or delete a policy. ● Modify or disable policies in a group. ● Apply policies to servers in batches on the **Servers** page.	×	√ (Only the default enterprise policy group is supported.)	√	√
	Security report	Check weekly or monthly server security trend, key security events, and risks.	×	√	√	√
Security configuration	2FA	Prevent brute-force attacks by using password and SMS/email authentication.	√	√	√	√
Web Tamper Protection	Static WTP	Static web page files on your website servers are protected from tampering.	×	×	×	√
	Net disk tampering prevention	Files in your net disks are protected from tampering.	×	×	×	√

Function	Item	Description	Basic	Enterprise	Premium	WTP
	Dynamic WTP	Dynamic web page files in your website databases are protected from tampering.	×	×	×	√

1.5 Scenarios

Security Compliance

The intrusion detection function of HSS protects accounts and systems on cloud servers, helping enterprises meet compliance standards.

Centralized Security Management

You can manage the security configurations and events of all your cloud servers on the HSS console, reducing risks and management costs.

Security Risk Evaluation

You can check and eliminate all the risks (such as risky accounts, open ports, software vulnerabilities, and weak passwords) on your servers.

Account Protection

Take advantage of comprehensive account security capabilities, including prevention, anti-attack, and post-attack scan. You can use 2FA to block brute-force attacks on accounts, enhancing the security of your cloud servers.

Proactive Security

Count and scan your server assets, check and fix vulnerabilities and unsafe settings, and proactively protect your network, applications, and files from attacks.

Intrusion Detection

Scan all possible attack vectors to detect and fight advanced persistent threats (APTs) and other threats in real time, protecting your system from their impact.

1.6 Constraints

Supported Server Types

- ECS

Supported OSs

HSS agents can run on Linux OSs, such as CentOS and EulerOS; and Windows OSs, such as Windows Server 2008, 2012, and 2016.

NOTICE

The agent is probably incompatible with the Linux or Windows OS versions that have reached end of life. To obtain better HSS service experience, you are advised to install or upgrade to an OS version supported by the agent.

- **Table 1-8** and **Table 1-9** list Linux OS versions supported by HSS.

  Table 1-8 Linux OS version (x86 computing)

No.	OS Version
1	CentOS: 6, 7 and 8 (64 bit)
2	Debian: 7, 8, 9, and 10 (32/64 bit)
3	EulerOS: 2.2, 2.3 and 2.5 (64 bit)
4	Fedora: 24, 25, and 30 (64 bit)
5	OpenSUSE: 13.2, 15.0 and 42.2 (64bit)
6	Ubuntu: 14.04, 16.04, and 18.04 (32/64 bit)
7	SUSE: 11 and 12 (64 bit) and SAP HANA
8	Gentoo: 13.0 and 17.0 (64 bit)
9	Oracle Linux: 6.9, 7.4 (64bit)

  Table 1-9 Linux OS version (Kunpeng computing)

No.	OS Version
1	CentOS: 7.4, 7.5, 7.6, 8.0 64bit with ARM (40 GB)
2	EulerOS: 2.8 64bit with ARM (40 GB)
3	Fedora: 29 64bit with ARM (40 GB)
4	OpenSUSE: 15.0 64bit with ARM (40 GB)
5	Ubuntu: 18.04 64bit with ARM (40 GB)

- **Table 1-10** lists Windows OS versions supported by HSS.

Table 1-10 Supported Windows OSs

No.	OS Version	Constraint
1	Windows Server 2019 Datacenter 64-bit English (40 GB)	If a piece of third-party security software, such as McAfee, has been installed on your server, stop the protection function on the software before installing an HSS agent. After you install the agent, you can re-enable the protection function on the software.
2	Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	
3	Windows Server 2016 Standard 64-bit English (40 GB)	
4	Windows Server 2016 Standard 64-bit Chinese (40 GB)	
5	Windows Server 2016 Datacenter 64-bit English (40 GB)	
6	Windows Server 2016 Datacenter 64-bit Chinese (40 GB)	
7	Windows Server 2012 R2 Standard 64-bit English (40 GB)	
8	Windows Server 2012 R2 Standard 64-bit Chinese (40 GB)	
9	Windows Server 2012 R2 Datacenter 64-bit English (40 GB)	
10	Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)	
11	Windows Server 2008 R2 Standard 64-bit English (40 GB)	
12	Windows Server 2008 R2 Standard 64-bit Chinese (40 GB)	
13	Windows Server 2008 R2 Datacenter 64-bit Chinese (40 GB)	
14	Windows Server 2008 R2 Enterprise 64-bit English (40 GB)	
15	Windows Server 2008 R2 Enterprise 64-bit Chinese (40 GB)	
16	Windows Server 2008 Web R2 64-bit Chinese (40 GB)	

1.7 HSS Permissions Management

If you need to assign different permissions to different employees in your enterprise to access HSS resources, IAM is a good choice for fine-grained

permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use HSS resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using HSS resources.

If your account does not need individual IAM users for permissions management, then you may skip over this chapter.

HSS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

HSS is a project-level service deployed and accessed in specific physical regions. To assign permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing HSS, the users need to switch to a region where they have been authorized to use cloud services.

You can grant users permissions by using roles and policies.

- Roles: A coarse-grained authorization mechanism provided by IAM to define permissions based on users' job responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you must also assign other roles on which the permissions depend to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- Policies: A fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant HSS users only the permissions for managing a certain type of resources. Most policies define permissions based on APIs. For the API actions supported by HSS, see **Permissions Policies and Supported Actions**.

Table 1-11 lists more details.

Table 1-11 System-defined permissions supported by HSS

Role/Policy Name	Description	Role/ Policy Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS.	System-defined role	• This role depends on the **Tenant Guest** role. **Tenant Guest**: a global role, which must be assigned in the Global project
HSS FullAccess	Full permissions for HSS	System-defined policy	None
HSS ReadOnlyAccess	Read-only permissions for HSS	System-defined policy	None

1.8 Related Services

HSS users can use SMN to receive alarm notifications, IAM service to manage user permissions, and Cloud Trace Service (CTS) to audit user behaviors.

Elastic Cloud Server (ECS)

HSS agents can be installed on ECSs.

- For details about ECS, see the *Elastic Cloud Server User Guide*.

Simple Message Notification (SMN)

SMN is an extensible, high-performance message processing service.

- To enable alarm notifications, you must configure SMN first.
- After the SMN is enabled, you will receive alarm notifications sent from HSS if your server is attacked or have high risks detected.
- On the **Alarm Notification** tab, you can configure **Daily Alarm Notification** and **Real-Time Alarm Notification** as required.

For details about SMN, see *Simple Message Notification User Guide*.

Identity and Access Management

IAM is a free identity management service that can implement refined user permission isolation and control based on user identities. It is the basic permission management service and can be used free of charge.

For details about IAM, see *Identity and Access Management User Guide*.

Cloud Trace Service (CTS)

CTS is a professional log audit service that records user operations in HSS. You can use the records for security analysis, compliance auditing, resource tracking, and fault locating. It is the basic log management service and can be used free of charge.

For details about CTS, see *Cloud Trace Service User Guide*.

1.9 Concepts

Account Cracking

Account cracking refers to the intruder behavior of guessing or cracking the password of an account.

Viewing Information About Weak Passwords

A weak password can be easily cracked.

Viewing Information About Malicious Programs

A malicious program, such as a backdoor, Trojan horse, worm, or virus, is developed with attack or illegal remote control intents.

Malware covertly inlays code into another program to run intrusive or disruptive programs and damage the security and integrity of the data on an infected server. Malware includes viruses, Trojan horses, and worms, classified by their ways of transmission.

HSS reports both identified and suspicious malware.

Ransomware

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.

Ransomware often uses a range of algorithms to encrypt the victim's files and demand a ransom payment to get the decryption key. Digital currencies such as Bitcoin are typically used for the ransoms, making tracing and prosecuting the attackers difficult.

Ransomware interrupts businesses and can cause serious economic losses. We need to know how it works and how we can prevent it.

Two-Factor Authentication

Two-factor authentication (2FA) refers to the authentication of user login by the combination of the user password and a verification code.

Web Tamper Protection

Web Tamper Protection (WTP) is an HSS edition that protects your files, such as web pages, documents, and images, in specific directories against tampering and sabotage from hackers and viruses.

Project

Projects are used to group and isolate OpenStack resources, including computing, storage, and network resources. A project can be a department or a project team.

Multiple projects can be created for one account.

2 Enabling HSS

2.1 Install an Agent

2.1.1 Installing an Agent on the Linux OS

You can enable HSS only after the HSS agent is installed on your servers. This topic describes how to install the agent on a server running a Linux OS. For details about how to install an agent on the Windows OS, see **Installing an Agent on the Windows OS**.

NOTE

WTP and HSS can use the same agent on a server.

Default Installation Path

The agent installation path on servers running the Linux OS cannot be customized. The default path is:

/usr/local/hostguard/

Prerequisites

- An EIP has been bound to the server on which the agent is to be installed.
- A remote management tool, such as Xftp, SecureFX, and WinSCP, has been installed on your PC.
- The Security-Enhanced Linux (SELinux) firewall has been disabled. The firewall affects agent installation and should remain disabled until the agent is installed.

Installing an Agent Using Commands

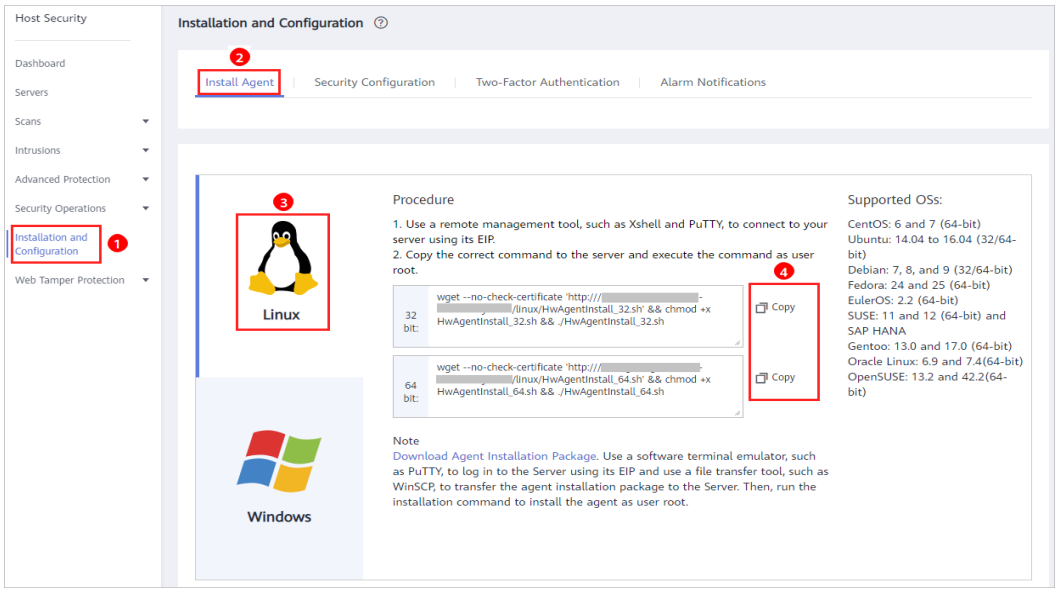
This procedure involves logging in to the server and running commands.

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** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Installation and Configuration**. On the **Install Agent** tab, copy the required installation command.

Figure 2-1 Copying the command for installing the agent



Step 4 Remotely log in to the server where the agent is to be installed.

- You can log in to the ECS management console and click **Remote Login** in the ECS list.
- If your server has an EIP bound, you can also use a remote management tool, such as Xftp, SecureFX, or WinSCP, to log in to the server and install the agent on the server as user **root**.

Step 5 Paste the copied installation command and press **Enter** to install the agent on the server.

If information similar to the following is displayed, the agent is successfully installed:

```
Preparing...                ########################################## [100%]
1:hostguard                 ########################################## [100%]
Hostguard is running.
Hostguard installed.
```

Step 6 Run the **service hostguard status** command to check the running status of the agent.

If the following information is displayed, the agent is running properly:

```
Hostguard is running
```

----End

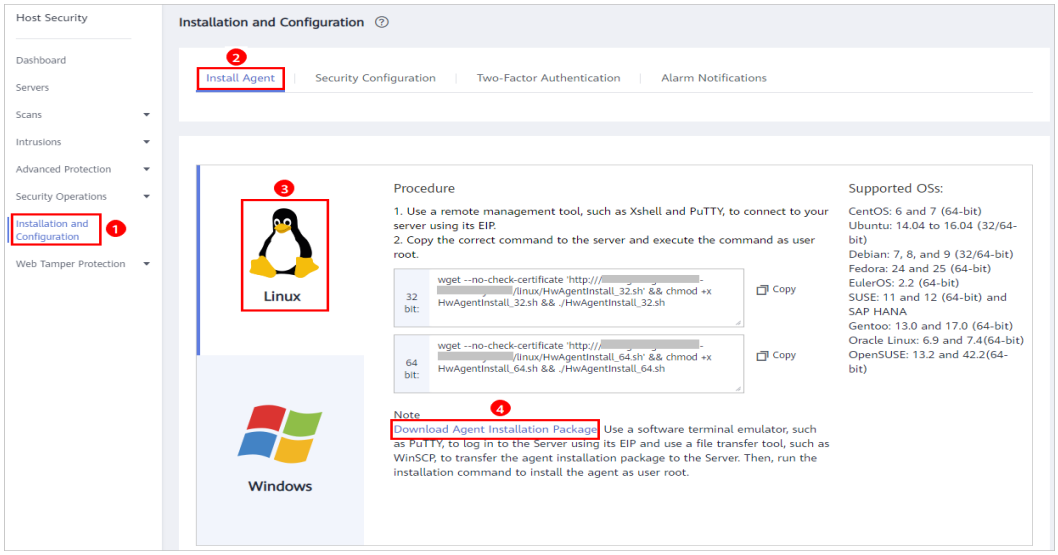
Installing an Agent Using an Installation Package

Download the agent installation package, upload it to the server where the agent is to be installed, and run the installation command on the server to install the agent.

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, choose **Installation and Configuration**. On the **Install Agent** tab, download the agent package.

Figure 2-2 Downloading the agent installation package



Step 3 Download the agent to be installed based on the server OS version.

Step 4 Use a file transfer tool, such as Xftp, SecureFX, or WinSCP, to upload the agent installation package to the server.

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

- You can log in to the ECS management console and click **Remote Login** in the ECS list.
- If your server has an EIP bound, you can also use a remote management tool, such as Xftp, SecureFX, or WinSCP, to log in to the server and install the agent on the server as user **root**.

Step 6 Run **cd** *Installation_package_directory* to access the directory.

Step 7 Run the following command to install the agent on the server:

- For an .rpm package, run **rpm -ivh** *Package_name*.

  NOTE

  To forcibly install the agent, run the **rpm -ivh --force** *Package_name* command.

- For a .deb package, run **dpkg -i** *Package_name*.

  If information similar to the following is displayed, the agent is successfully installed:

```
Preparing...                ########################################### [100%]
1:hostguard                 ########################################### [100%]
```

```
Hostguard is running.
Hostguard installed.
```

Step 8 Run the **service hostguard status** command to check the running status of the agent.

If the following information is displayed, the agent is running properly:

```
Hostguard is running
```

----End

2.1.2 Installing an Agent on the Windows OS

You can enable HSS only after an HSS agent is installed on the servers. This topic describes how to install the agent on a server running a Windows OS. For details about how to install an agent on the Linux OS, see **Installing an Agent on the Linux OS**.

NOTE

WTP and HSS can use the same agent on a server.

Default Installation Path

The agent installation path on servers running the Windows OS cannot be customized. The default path is:

C:\Program Files (x86)\HostGuard

Prerequisites

- An EIP has been bound to the server on which the agent is to be installed.
- A remote management tool, such as pcAnywhere and UltraVNC, has been installed on your PC.

Procedure

There are two ways to install an agent. This section describes the first one.

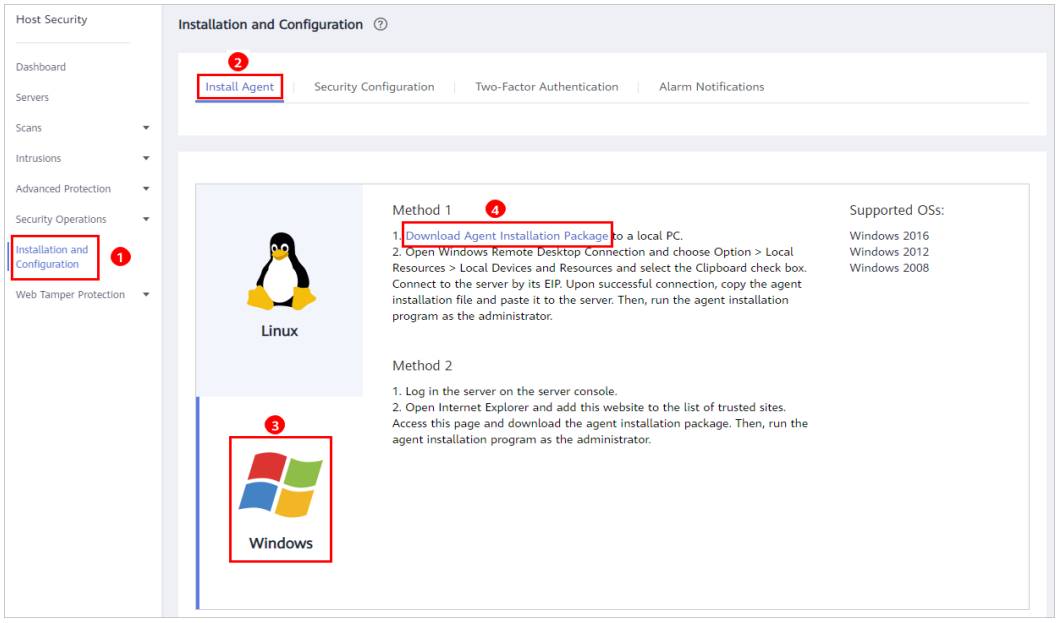
- Method 1: Download the agent installation package, upload it to the server where the agent is to be installed, and run the installation command on the server to install the agent.
- Method 2: Log in to the server where the agent is to be installed, log in to the management console using the server, and download and install 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** > **Host Security Service**.

Step 3 In the navigation pane on the left, choose **Installation and Configuration**. On the **Install Agent** tab, download the agent package.

Figure 2-3 Installing a Windows agent



Step 4 Remotely log in to the server where the agent is to be installed.

- You can log in to the ECS management console and click **Remote Login** in the ECS list.
- If an EIP has been bound to the server, you can use Windows Remote Desktop Connection or a third-party remote management tool, such as pcAnywhere and UltraVNC, to log in to the server and install the agent on the server as an administrator.

Step 5 Upload the agent installation package to the server where the agent is to be installed.

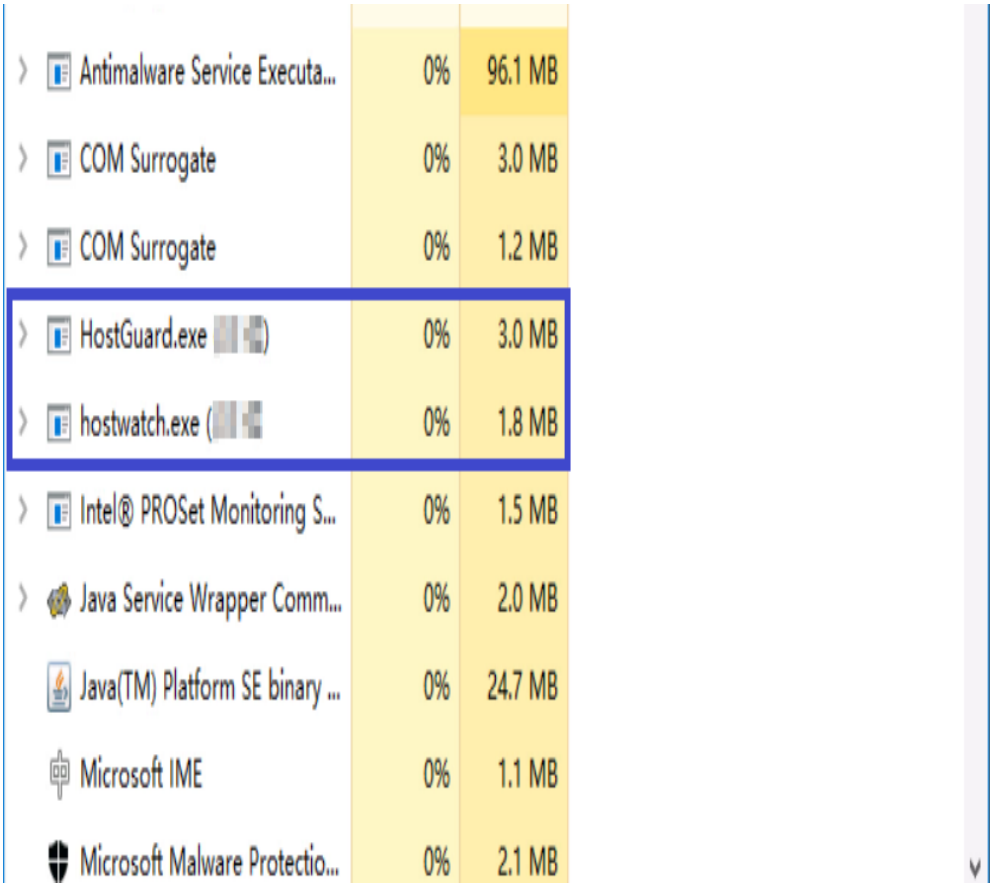
Step 6 Run the agent installation program as an administrator.

Select a host type on the **Select host type** page.

Step 7 Check the **HostGuard.exe** and **HostWatch.exe** processes in the Windows Task Manager.

If the processes do not exist, the agent installation fails. In this case, reinstall the agent.

Figure 2-4 Checking the agent status



----End

2.2 Set Alarm Notifications

2.2.1 Enabling Alarm Notification for the Basic/Enterprise/ Premium Edition

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 intercepted. If you do not receive any alarm notifications, view them in the message interception area.

Prerequisites

Before setting alarm notifications, you are advised to create a message topic in SMN as an administrator.

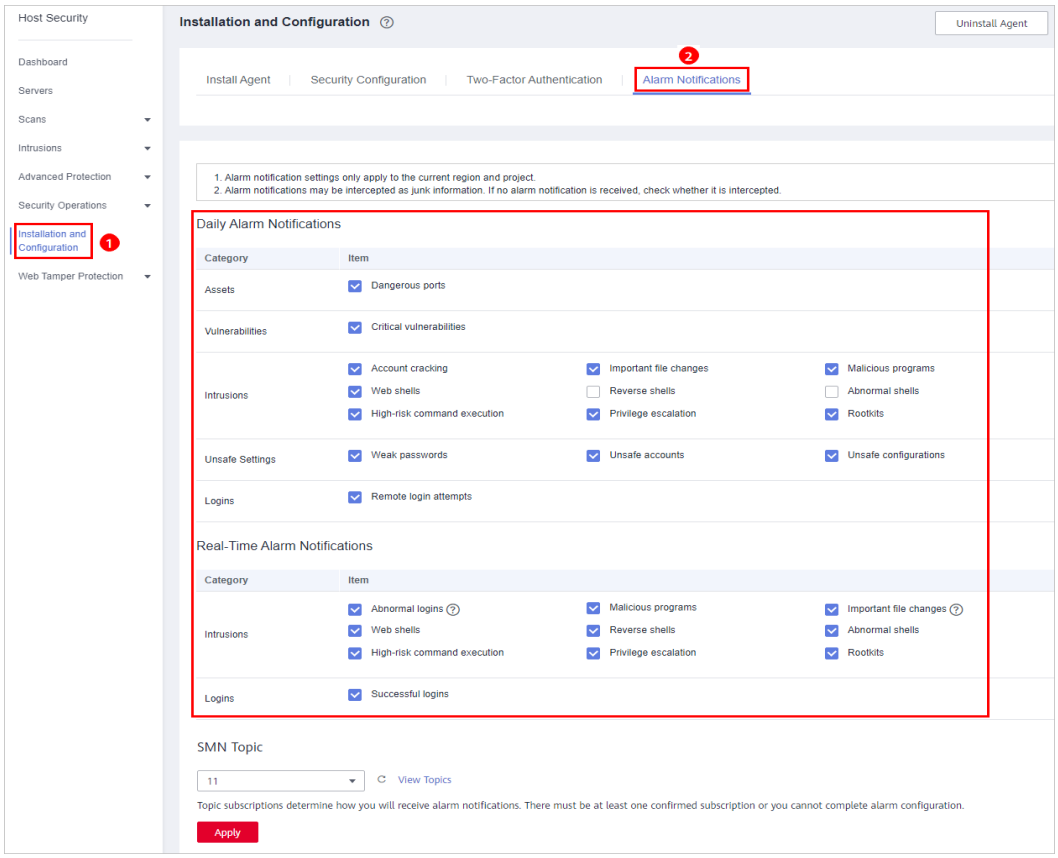
Enabling Alarm Notification for the Basic, Enterprise, or Premium Edition

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** > **Host Security Service**.

Step 3 On the displayed page, click the **Alarm Notifications** tab.

Figure 2-5 Basic/Enterprise/Premium edition



Step 4 Select the notification items for **Daily Alarm Notifications** and **Real-Time Alarm Notifications** as desired. For more information, see **Alarm Notifications**.

Table 2-1 Notification types

Notification Type	Description	Suggestion on Selecting a Notification Item
Daily alarm notification	The HSS system 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 SMN.	• 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, HSS sends alarms to the recipients you set in SMN.	• 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**.

Step 5 Select a message notification topic.

You can select an existing topic or click **View Topics** to create a topic.

- Multiple subscriptions can be added to a topic. Before selecting a topic, ensure that subscriptions added to it are in **Confirmed** status. Otherwise, notifications may fail to be received.
- 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.
- For details about topics and subscriptions, see *Simple Message Notification User Guide*.

Step 6 Click **Apply**.

----End

Alarm Notifications

Notification Type	Item	Description
Daily Alarm Notifications HSS 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.		
Assets	Dangerous port	Check for high-risk open ports and unnecessary ports.
Vulnerabilities	Critical vulnerabilities	Detect critical vulnerabilities and fix them in a timely manner.
Intrusions	Account cracking	Detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts. • If the number of brute-force attacks from an IP address reaches 5 within 30 seconds, the IP address will be blocked. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. • You can check whether the 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.
	Important file changes	HSS only checks whether directories or files have been modified, not whether they are modified manually or by a process.
	Malicious programs	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.
	Web shells	Check whether the files (often PHP and JSP files) in your web directories are web shells.
	Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections.

Notification Type	Item	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.
	High-risk command execution	HSS checks executed commands in real time and generates alarms if high-risk commands are detected.
	Privilege escalation	HSS detects privilege escalation for processes and files in the current system.
	Rootkits	HSS detects suspicious rootkit installation in a timely manner by checking:
Unsafe Settings	Weak passwords	Detect weak passwords in MySQL, FTP, and system accounts.
	Unsafe accounts	Check for suspicious and unnecessary accounts on the servers to prevent unauthorized access and operations.
	Unsafe configurations	Detect unsafe settings of key applications that will probably be exploited by hackers to intrude servers.
Logins	Remote login attempts	Check and handle remote logins. If a user's login location is not any common login location you set, an alarm will be triggered.
Real-Time Alarm Notifications When an event occurs, an alarm notification is immediately sent.		
Intrusions	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.
	Malicious programs	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.
	Important file changes	HSS only checks whether directories or files have been modified, not whether they are modified manually or by a process.
	Web shells	Check whether the files (often PHP and JSP files) in your web directories are web shells.

Notification Type	Item	Description
	Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections.
	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.
	High-risk command execution	HSS checks executed commands in real time and generates alarms if high-risk commands are detected.
	Privilege escalation	HSS detects privilege escalation for processes and files in the current system.
	Rootkits	HSS detects suspicious rootkit installation in a timely manner by checking:
Logins	Successful logins	This alarm does not necessarily indicate a security issue. If you have selected **Successful logins** in the **Real-Time Alarm Notifications** area, HSS will send alarms when detecting any successful logins. If all the accounts on your HSS are managed by a single administrator, such alarms help them conveniently monitor system accounts. If the system accounts are managed by multiple administrators, or different servers are managed by different administrators, too many alarms will interrupt O&M personnel. In this case, you are advised to disable the alarm item. **NOTE** Alarms on this event do not necessarily indicate attacks. Logins from valid IP addresses are not attacks.

2.2.2 Enabling Alarm Notification for the WTP Edition

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 intercepted. If you do not receive any alarm notifications, view them in the message interception area.

Prerequisites

Before setting alarm notifications, you are advised to create a message topic in SMN as an administrator.

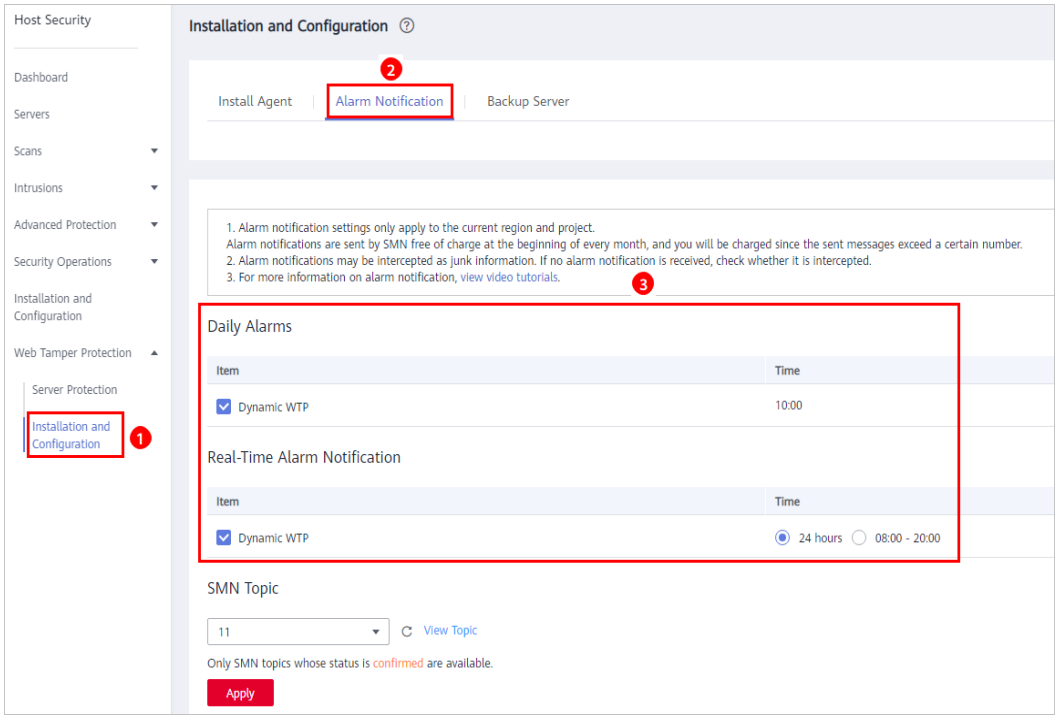
Enabling WTP Alarm Notifications

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** > **Host Security Service**.

Step 3 Configure alarm time on the **Alarm Notification** tab of WTP.

Figure 2-6 Configuring alarm notifications



Step 4 Select a message notification topic.

You can select an existing topic or click **View Topics** to create a topic.

- Multiple subscriptions can be added to a topic. Before selecting a topic, ensure that subscriptions added to it are in **Confirmed** status. Otherwise, notifications may fail to be received.
- 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.
- For details about topics and subscriptions, see *Simple Message Notification User Guide*.

Step 5 Click **Apply**.

----End

2.3 Enable Server Protection

2.3.1 Enabling the Basic/Enterprise/Premium Edition

For the WTP edition, choose **Web Tamper Protection** > **Server Protection** and then enable it. For details, see **Enabling the WTP Edition**.

Check Mode

The HSS system detects all data at 00:00 every day.

If you enable server protection before the detection interval, you can view detection results only after the detection is performed at 00:00 of the next day or you perform a manual detection immediately.

Prerequisites

- In the server list on the **Servers** page of the HSS console, the **Agent Status** of the target server is **Online**.
- Alarm notifications have been enabled.
- To better protect your containers, you are advised to **set security configurations**.

Constraints

- Linux OS

  On servers running the EulerOS with ARM, HSS does not block the IP addresses suspected of SSH brute-force attacks, but only generates alarms.
- Windows OS
  - Authorize the Windows firewall when you enable protection for a Windows server. Do not disable the Windows firewall during the HSS in-service period. If the Windows firewall is disabled, HSS cannot block brute-force attack IP addresses.
  - If the Windows firewall is manually enabled, HSS may also fail to block brute-force attack IP addresses.

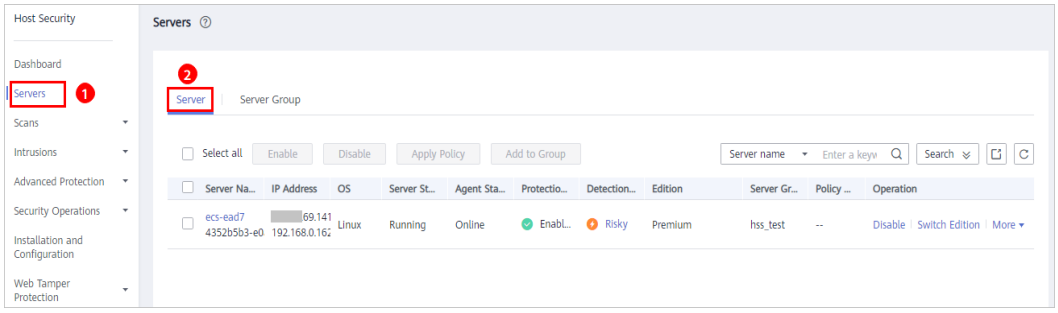
Enabling Protection

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** > **Host Security Service**.

Step 3 In the navigation tree on the left, choose **Servers**.

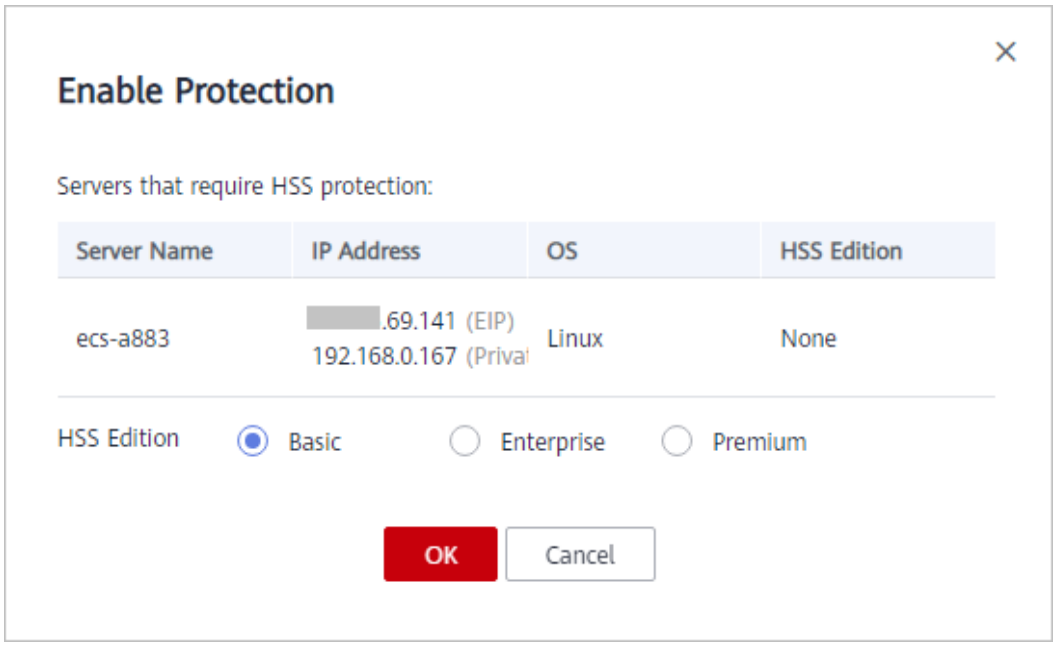
Figure 2-7 Server list



Step 4 Select the target server and click **Enable**.

In the **Enable Protection** dialog box, select the HSS edition, as shown in **Figure 2-8**.

Figure 2-8 Enabling HSS



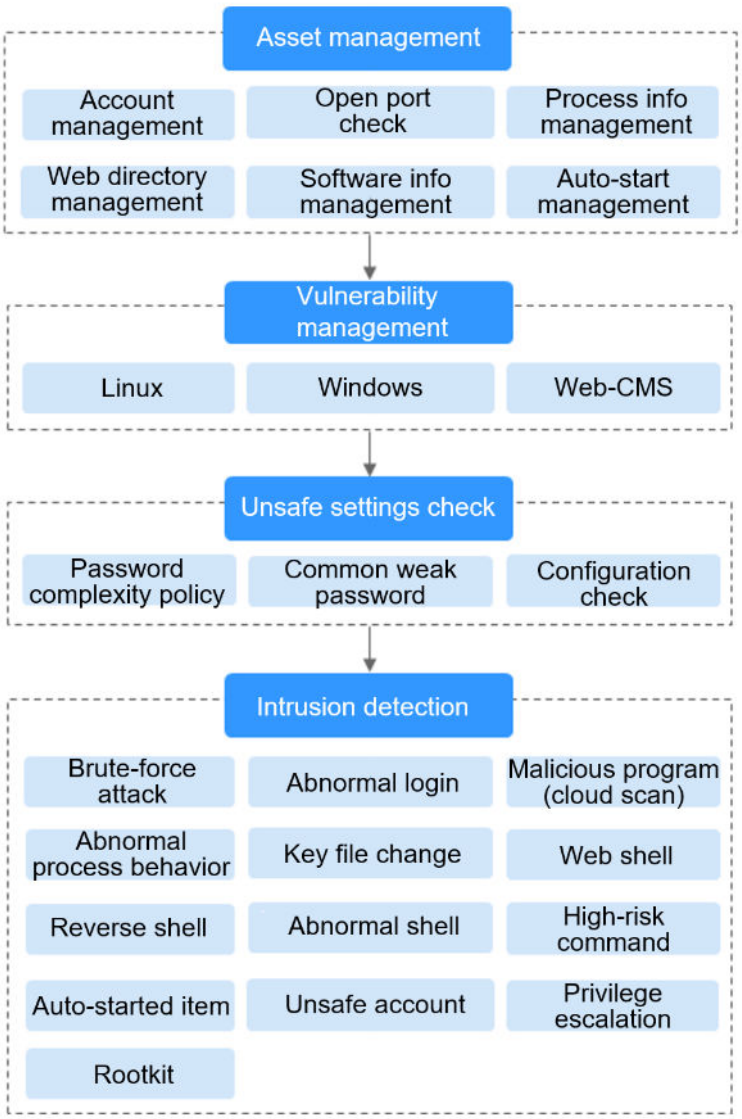
Step 5 Click **OK**. View the server protection status in the server list.

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

After HSS is enabled, it will scan your servers for security issues. Check items vary according to the edition you enabled. **Figure 2-9** illustrates more details.

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

Figure 2-9 Automatic security check items



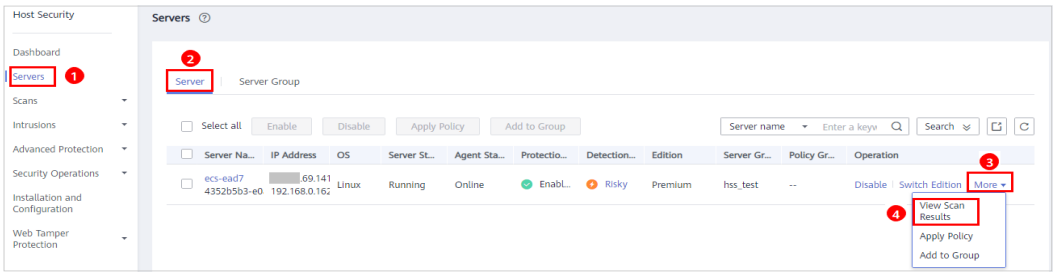
----End

Viewing Detection Details

After server protection is enabled, HSS will immediately perform comprehensive detection on the server. The detection may take a long time, which needs your patience.

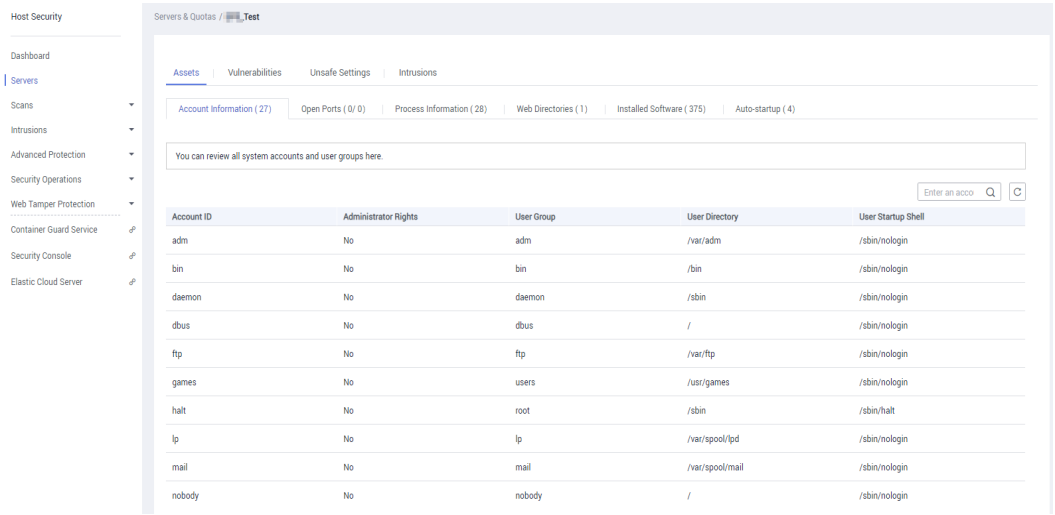
In the **Operation** column on the **Server** tab, choose **More** > **View Scan Results** to view the detection result of a specified server.

Figure 2-10 Viewing details



The details page shows detection results and detected risks.

Figure 2-11 Viewing the detection result



Switching Editions

You can switch between the basic, enterprise, and premium editions of HSS if you already purchased quotas of the required editions.

NOTICE

- If the HSS service is switched from a higher edition to a lower edition, protected servers will be more vulnerable to attacks.
- You can switch from other editions to the basic, enterprise, or premium edition.

- Preparations
  - Before switching to a lower edition, check the server, handle known risks, and record operation information to prevent O&M errors and attacks.
- Operations after the edition change
  - 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.

Follow-up Operation

You can manually configure check items, as shown in **Figure 2-12**. Configurable items vary according to the edition you enabled.

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

Figure 2-12 Manual check items

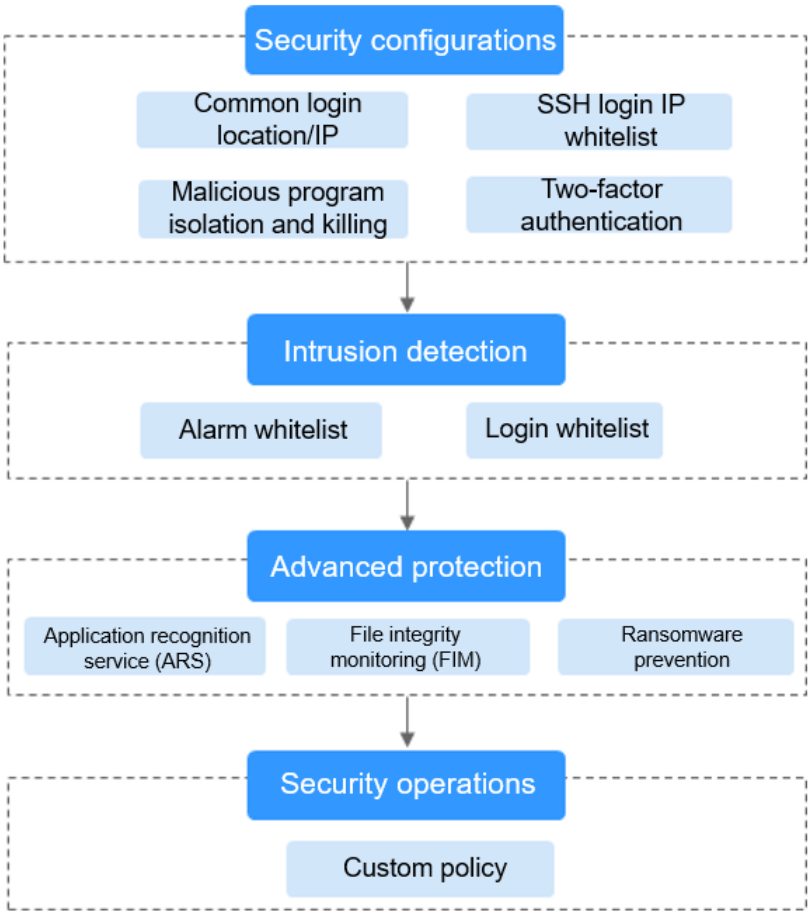


Table 2-2 Manual check items

Function	Check Item	Reference
Security configuration	• Common login location/IP address • SSH login IP address whitelist • Isolating and killing malicious programs	**Security Configuration**

Function	Check Item	Reference
Intrusion detection	• Alarm whitelist • Login whitelist	Intrusion Detection
Advanced protection	• Application recognition service (ARS) • File integrity monitoring (FIM) • Ransomware prevention	Advanced Protection
Security operations	• Custom policy management	Security Operations

Follow-Up Procedure

Disabling HSS

On the **Server** tab of the **Servers** page, click **Disable** in the **Operation** column of a server.

NOTICE

- Before disabling protection, perform a comprehensive detection on the server, handle known risks, and record operation information to prevent O&M errors and attacks on the server.
- After protection is disabled, 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.

2.3.2 Enabling the WTP Edition

The premium edition will be enabled when you enable WTP.

How WTP Prevents Web Page Tampering

Table 2-3 Protection mechanisms

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 a protected directory is tampered with, it immediately uses the backup file on the local host to restore the file. 3. Remote backup and restoration If a file directory or backup directory on the local host is invalid, you can use the remote backup service to restore the tampered web page.
Dynamic web page protection	1. Malicious behavior filtering based on RASP The runtime application self-protection (RASP) technologies detect program behaviors, preventing attackers from tampering with web pages through application programs. 2. Network disk file access control WTP implements fine-grained management to control permissions for adding, modifying, and querying file content in network disks, preventing tampering without affecting website content release.

Restrictions

The Windows firewall must be enabled when you enable protection for a Windows server. Do not disable the Windows firewall during the HSS in-service period.

Prerequisites

- On the **Server Protection** page of the WTP console, the **Agent Status** of the target server is **Online**, and the **Protection Status** of the server is **Disabled**.
- In the server list on the **Servers** page of the HSS console, the **Agent Status** of the target server is **Online**, and the **Protection Status** of the server is **Disabled**.

Setting Protected Directories

You can set:

- Directories

  You can add a maximum of 50 protected directories to a host. For details, see **Adding a Protected Directory or File System**.

To record the running status of the server in real time, exclude the log files in the protected directory. You can grant high read and write permissions for log files to prevent attackers from viewing or tampering with the log files.

- File systems

  You can add a maximum of five file systems. For details, see **Adding a Protected Directory or File System**.

  OS partitions are not allowed.

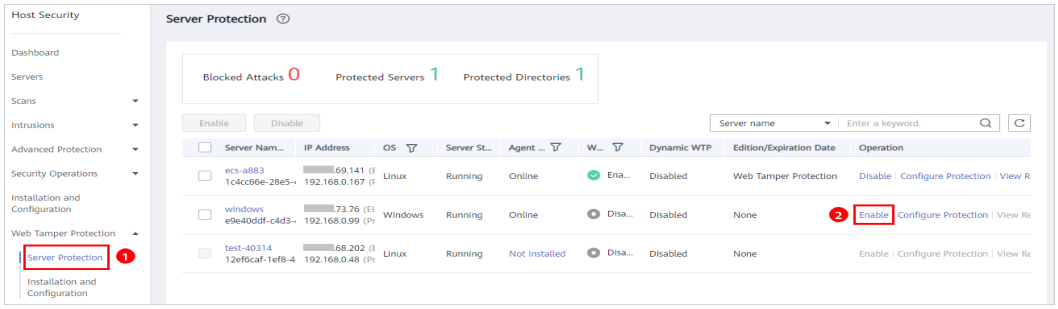
Enabling WTP

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** > **Host Security Service**.

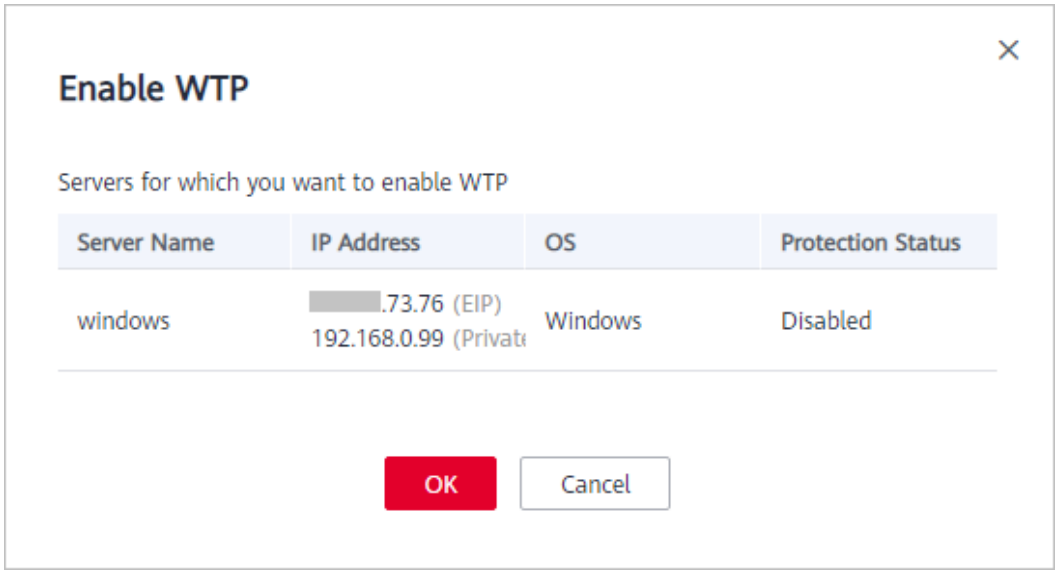
Step 3 In the navigation pane, choose **Web Tamper Protection** > **Server Protection**. Click **Enable** in the **Operation** column of a server.

Figure 2-13 Web Tamper Protection



Step 4 In the **Enable WTP** dialog box, click **OK**, as shown in **Figure 2-14**.

Figure 2-14 Enabling WTP



Step 5 View the server status on the **Web Tamper Protection** page.

----End

NOTICE

- Disable WTP before updating a website and enable it after the update is complete. Otherwise, the website will fail to be updated.
- Your website is not protected while WTP is disabled. Enable it immediately after updating your website.

Follow-Up Procedure

Disabling WTP

Choose **Web Tamper Protection** > **Server Protection** and click **Disable** in the **Operation** column of a server.

NOTICE

- Before disabling WTP, perform a comprehensive detection on the server, handle known risks, and record operation information to prevent O&M errors and attacks on the server.
- If WTP is disabled, web applications are more likely to be tampered with. Therefore, you need to delete important data on the server, stop important services on the server, and disconnect the server from the external network in a timely manner to avoid unnecessary losses caused by attacks on the server.
- After you or disable WTP, files in the protected directory are no longer protected. You are advised to process files in the protected directory before performing these operations.
- If you find some files missing after disabling WTP, search for them in the local or remote backup path.

3 Viewing the Server List

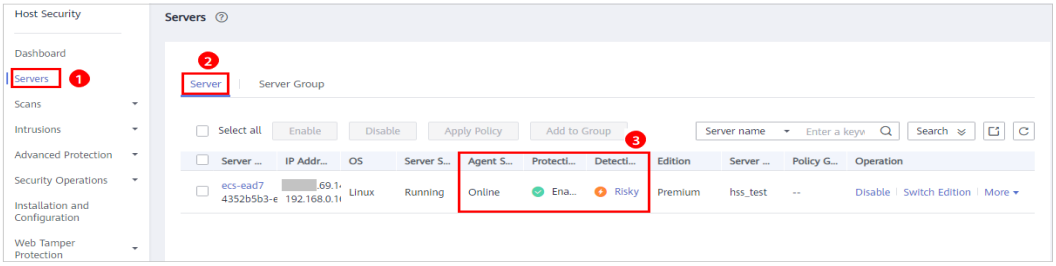
Viewing the Server List of the Basic/Enterprise/Premium Edition

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** > **Host Security Service**.

Step 3 On the **Server** tab, check the protection status of servers.

Figure 3-1 Server list



NOTE

- You can search for a server by its name, EIP, or private IP address.
- You can expand the advanced search area and search for a server by its name, ID, IP address, OS, agent status, protection status, detection result, policy group, server group, edition, or server status.
- To export the server list, click .

Table 3-1 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. • **Online**: The agent is running properly. • **Offline**: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers. You can click **Offline**, and view servers whose agents are offline and the offline reasons at the bottom of the page that is displayed.
Protection Status	• **Enabled**: The server is fully protected by HSS. • **Disabled**: The server is not protected. If a server does not need protection, you can disable HSS for it to reduce its resource consumption.
Detection Result	• **Risky**: The host has risks. • **Safe**: No risks are found. • **Pending risk detection**: HSS is not enabled for the server.

----End

Viewing the WTP 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** > **Host Security Service**.

Step 3 Choose **Web Tamper Protection** > **Server Protection**. Check the protection status of servers.

Figure 3-2 Server protection

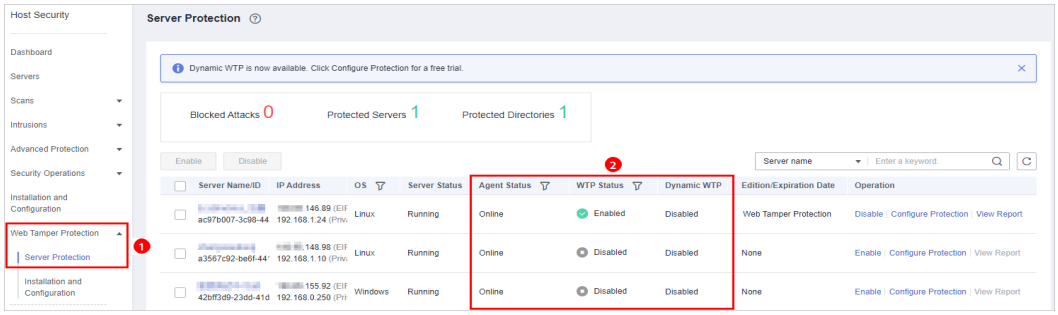


Table 3-2 Statuses

Parameter	Description
Agent Status	• **Not installed**: The agent has not been installed or successfully started. Click **Not installed** and install the agent as prompted. • **Online**: The agent is running properly. • **Offline**: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers. You can click **Offline**, and view servers whose agents are offline and the offline reasons at the bottom of the page that is displayed.
WTP Status	Status of static WTP, which can be: • **Enabled**: HSS provides static WTP for the server. • **Scheduled protection**: WTP is disabled for the server in a certain period. To set this period, click **Configure Protection** in the **Operation** column, and click the **Scheduled Protection** tab. For more information, see **Setting Scheduled WTP Protection**. • **Disabled**: The server is not protected. If a server does not need static WTP, you can disable HSS for it to reduce its resource consumption.
Dynamic WTP	Status of dynamic WTP, which can be: • **Enabled**: Dynamic WTP is enabled for the server. To enable dynamic WTP, click **Configure Protection** in the **Operation** column, and click the **Dynamic WTP** tab. For more information, see **Enabling Dynamic WTP**. • **Enabled but not in effect**: Dynamic WTP is enabled but has not taken effect. You need to restart Tomcat to make it take effect. • **Disabled**: Dynamic WTP is disabled.

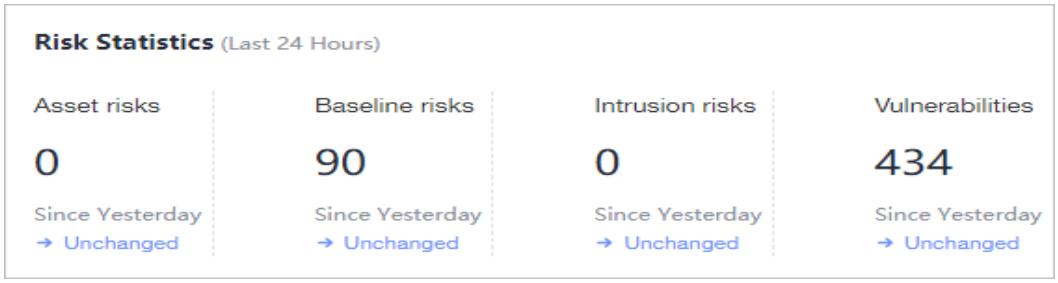
----End

4 Dashboard

The **Dashboard** page provides visibility into the protection status of cloud servers, risk statistics on protected servers within the last 24 hours, risk statistics of the last week, and top 5 vulnerable servers of the last week.

Risk Statistics on Protected Servers (Last 24 Hours)

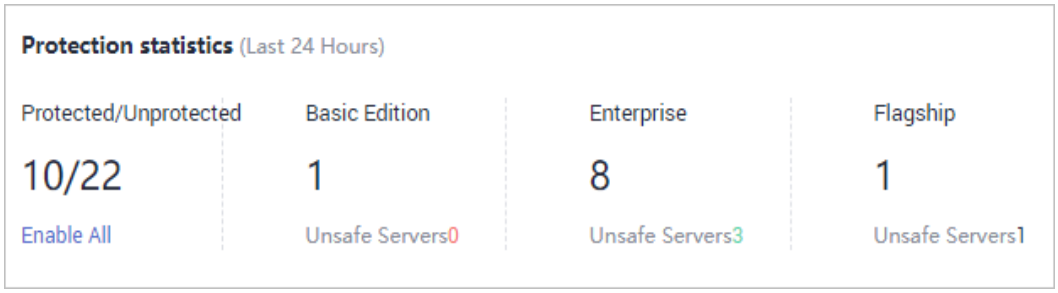
Figure 4-1 Risk statistics on protected servers (last 24 hours)



You can check the number of risks detected for protected servers over the past 24 hours.

Server Protection Status (Last 24 Hours)

Figure 4-2 Server protection status

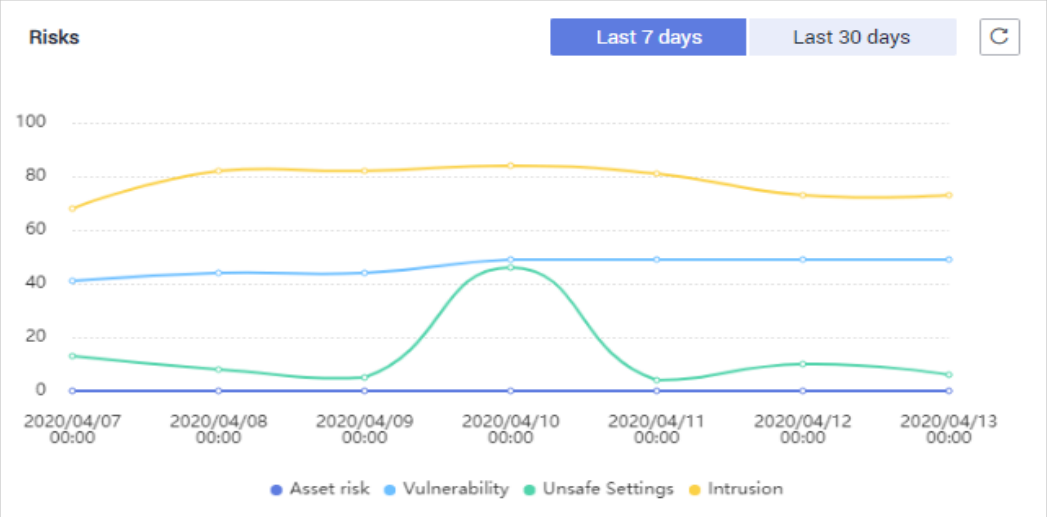


You can check the numbers of servers protected with the basic, enterprise, or premium edition and the number of unprotected servers.

To enable protection for required servers, click **Enable All**.

Risks

Figure 4-3 Risks



You can check risk statistics in the last 7 days or 30 days.

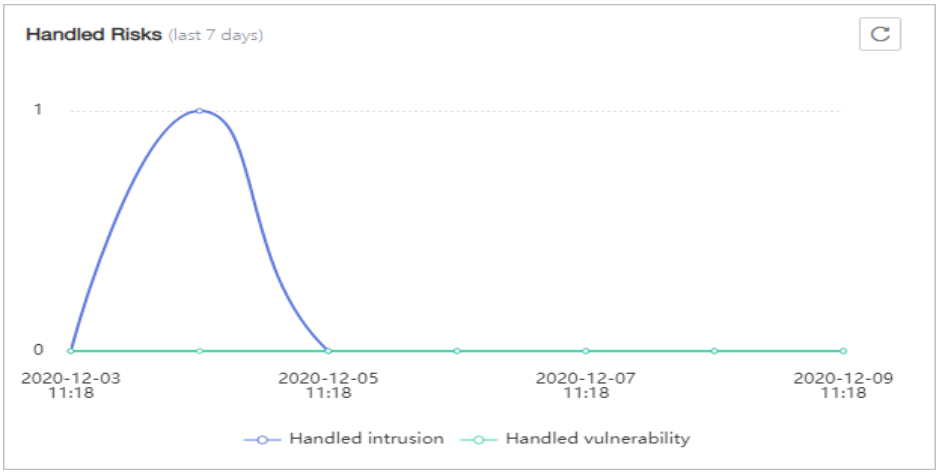
Table 4-1 Risks

Category	Item
Asset	• Account • Open port • Process • Web directory • Software • Auto-startup
Vulnerability	• Linux vulnerability • Windows vulnerability • Web-CMS vulnerability
Unsafe setting	• Password complexity policy • Common weak password • Unsafe configuration item

Category	Item
Intrusion	• Attacker IP address • Abnormal shell • Malicious program • High-risk command • Abnormal process behavior • Auto-startup check • Abnormal login • Privilege escalation • Changes in critical file • High-risk malicious program • Rootkit • Web shell • Unsafe account • Reverse shell

Handled Risks (Last 7 Days)

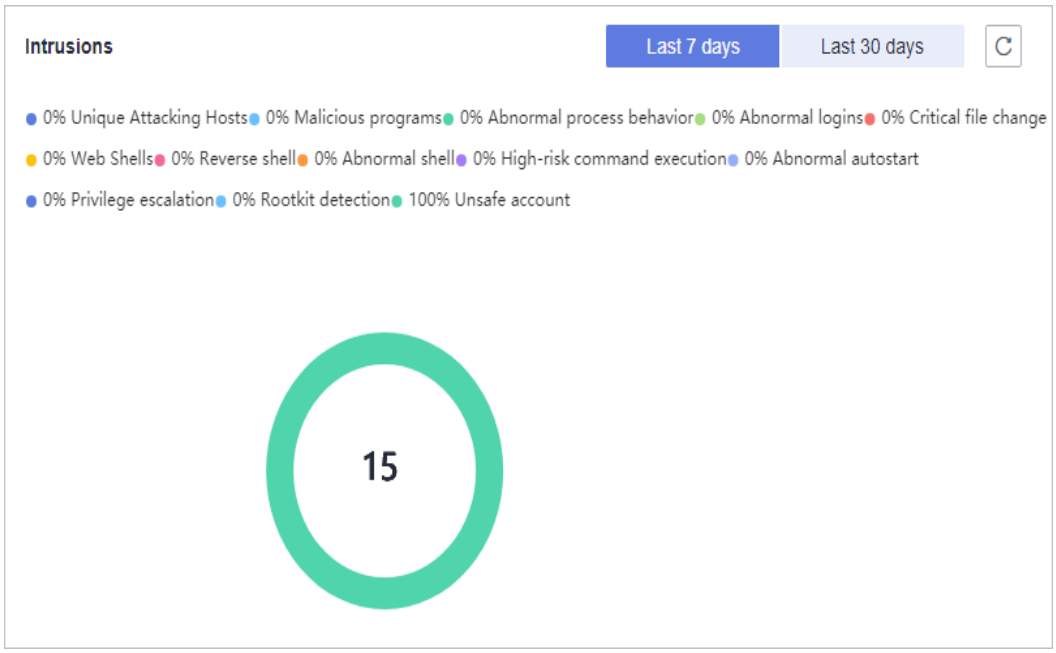
Figure 4-4 Handled risks



You can check the intrusions and vulnerabilities handled in the last seven days.

Intrusions

Figure 4-5 Intrusions



You can check the numbers and types of intrusions in the last seven or 30 days.

These intrusion statistics are updated at 00:00 a.m. every day.

Top 5 Unsafe Servers (Last 7 Days)

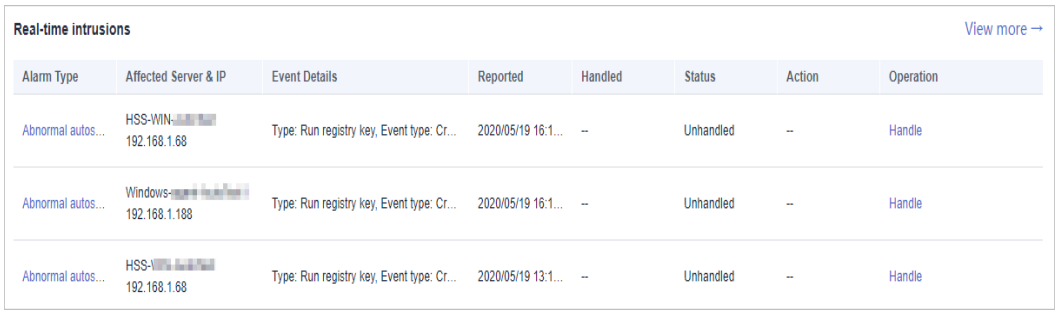
Figure 4-6 Top 5 unsafe servers (last 7 days)

If you have enabled the basic, enterprise, or premium edition HSS, you can check the top 5 unsafe servers, which have the most risks detected in the past week, and the numbers of each type of risks.

At 00:00 every morning, server risks and the five servers with highest risks in the past seven days are updated.

Real-time Intrusions

Figure 4-7 Real-time intrusions



You can check the latest five intrusion events that have not been processed in the last 24 hours, including their alarm names, affected server names/IP addresses, description, occurrence time, and status.

- To check alarm details, click an alarm name.
- To handle an alarm, click **Handle** in the **Operation** column of the alarm. After the alarm is handled, it will be removed from the list. The list refreshes and displays the latest five intrusion events that have not been handled in the last seven days.
- To check more alarm events, click **View more** to go to the **Events** page.

5 Security Configuration

After protection is enabled, you can set security configurations, including common login locations, common login IP addresses, SSH login IP address whitelist, and the automatic isolation and killing of 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** > **Host Security Service**.

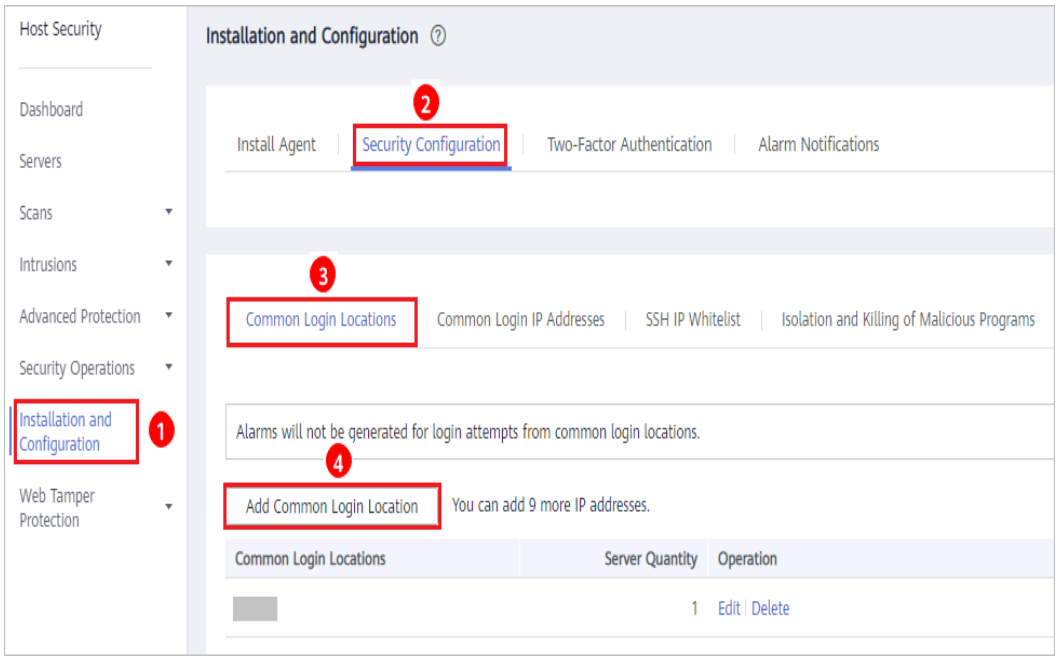
----End

Configuring Common Login Locations

After you configure common login locations, HSS will generate alarms on the logins from other login locations. A server can be added to multiple login locations.

Step 1 On the **Common Login Locations** tab, click **Add Common Login Location**.

Figure 5-1 Adding a common login location



Step 2 In the displayed dialog box, set the location and servers.

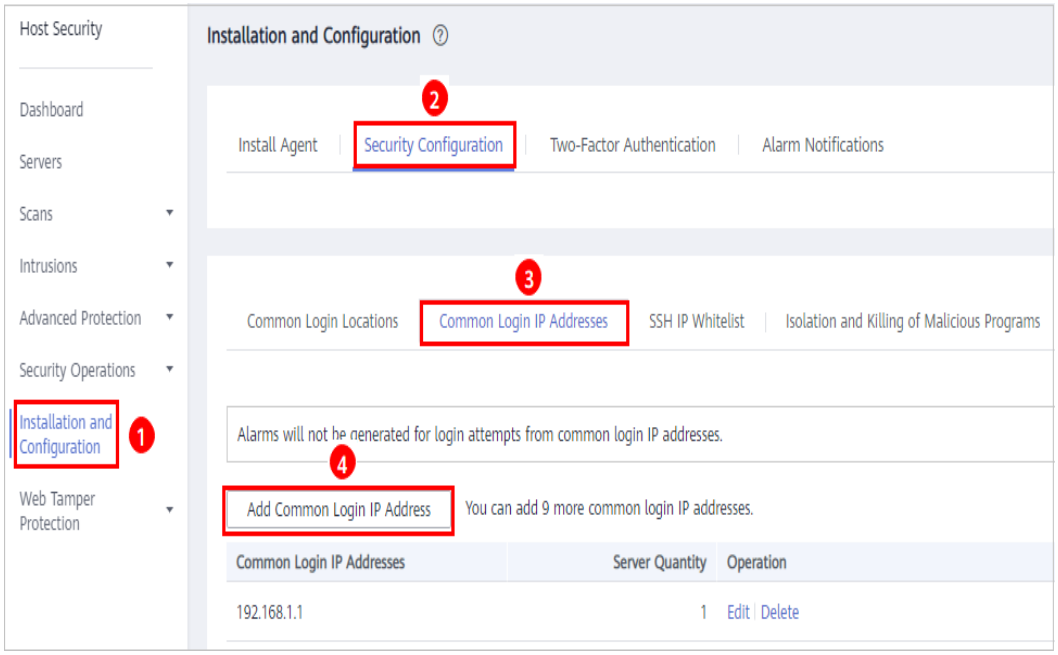
----End

Configuring Common Login IP Addresses

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

Step 1 On the **Common Login IP Addresses** tab, click **Add Common Login IP Address**.

Figure 5-2 Adding a common login IP address



Step 2 In the displayed dialog box, set the login IP address and servers.

NOTE

A common login IP address must be a public IP address or IP address segment. Otherwise, you cannot remotely log in to the server in SSH mode.

----End

Configuring an SSH Login IP Address Whitelist

The SSH login whitelist controls SSH access to servers, effectively preventing account cracking.

After you configure an SSH login IP address whitelist, SSH logins will be allowed only from whitelisted IP addresses.

- Before enabling this function, ensure that all IP addresses that need to initiate SSH logins are added to the whitelist. Otherwise, you cannot remotely log in to your server using SSH.

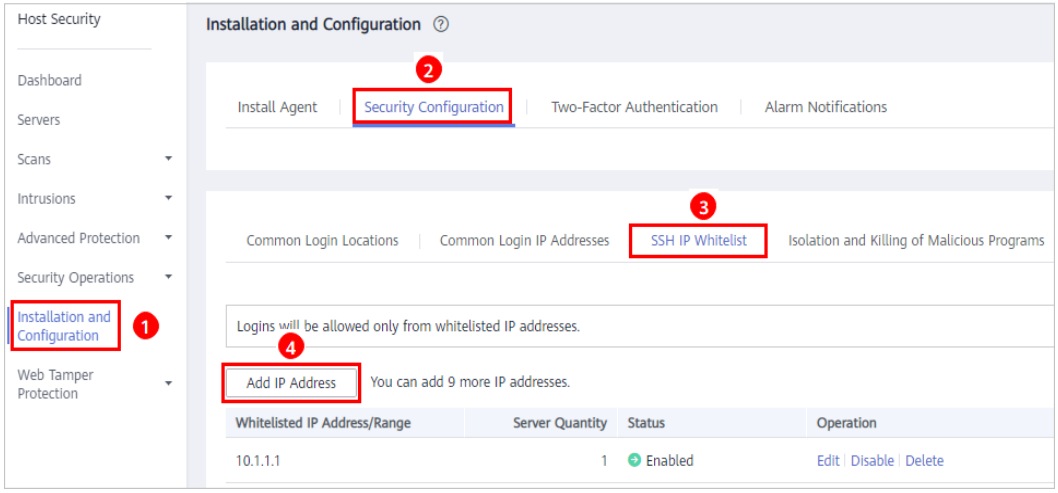
  If your service needs to access a server, but not necessarily via SSH, you do not need to add its IP address to the whitelist.
- Exercise caution when adding an IP address to the whitelist. This will make HSS no longer restrict access from this IP address to your servers.

NOTE

The SSH IP address whitelist does not take effect for servers running Kunpeng EulerOS (EulerOS with ARM).

Step 1 On the **SSH IP Whitelist** tab, click **Add IP Whitelist**.

Figure 5-3 Adding an SSH login IP address to whitelist



Step 2 In the **Add IP Whitelist** dialog box, enter an IP address and select servers.

NOTE

A whitelisted IP address must be a public IP address or IP address segment (IPv4 and IPv6 addresses are supported). Otherwise, you cannot remotely log in to the server in SSH mode.

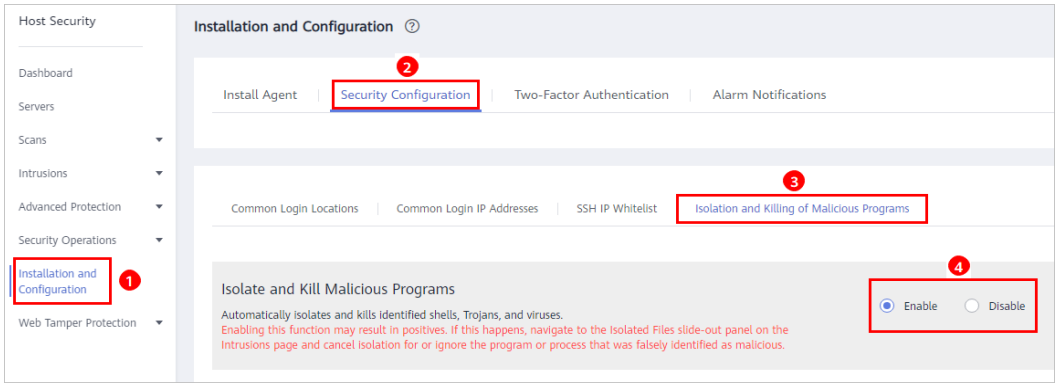
----End

Isolating and Killing Malicious Programs

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

On the **Isolation and Killing of Malicious Programs** tab, select **Enable**.

Figure 5-4 Isolating and killing malicious programs



Automatic isolation and killing may cause false positives. You can choose **Intrusions** > **Events** to view isolated malicious programs. You can cancel the isolation or ignore misreported malicious programs. For details, see **Checking and Handling Intrusion Events**.

NOTICE

- 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 **Intrusions** > **Events** and click **Malicious program (cloud scan)**.

Enabling 2FA

- 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

- You have created a message topic whose protocol is SMS or email.
- Server protection has been enabled.
- Linux servers require user passwords for login.

- To enable two-factor authentication, 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.

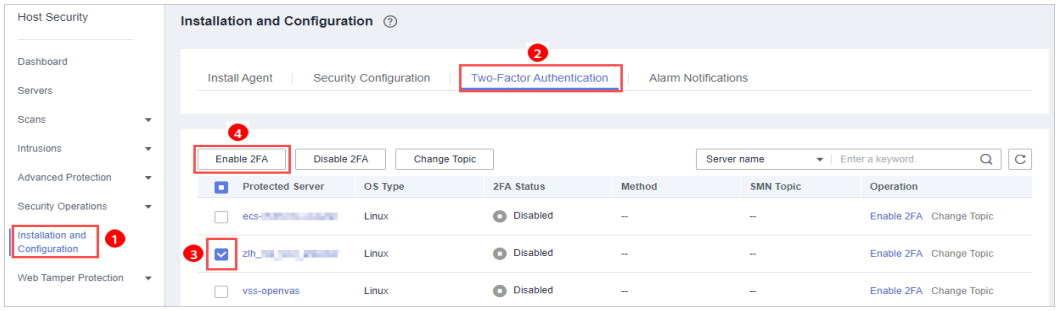
Constraints and Limitations

- If 2FA is enabled, you cannot log in to the servers running a GUI Linux OS.

Procedure

Step 1 On the **Two-Factor Authentication** tab, click **Enable 2FA**.

Figure 5-5 2FA



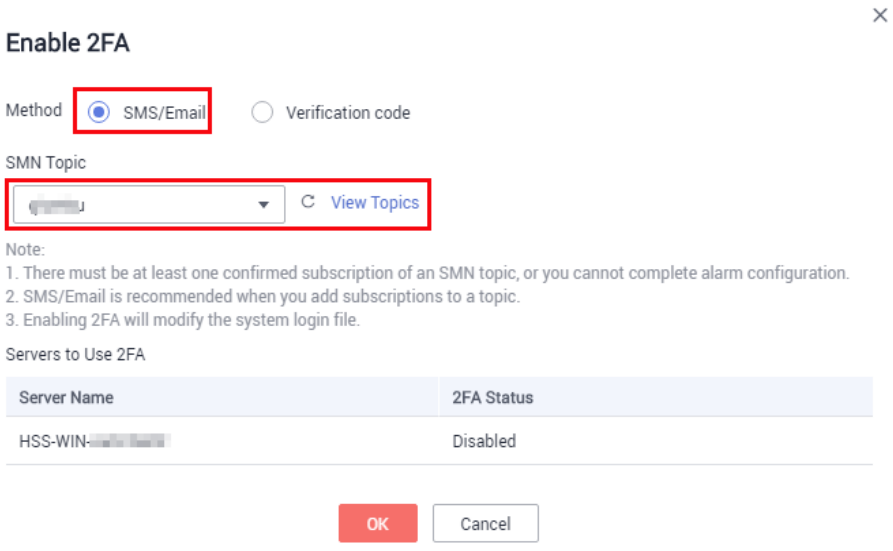
Step 2 In the displayed **Enable 2FA** dialog box, select an authentication mode.

- **SMS/Email**

  You need to select an SMN topic for SMS and email verification.

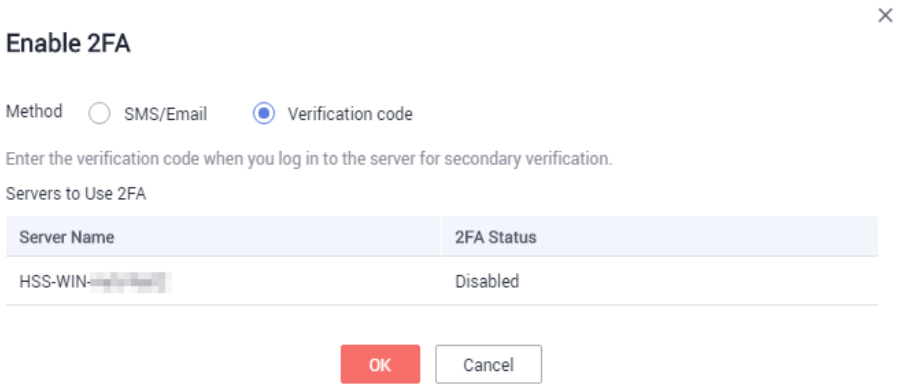
  - The drop-down list displays only notification topics that have been confirmed.
  - If there is no topic, click **View** to create one.
  - During authentication, all the mobile numbers and email addresses specified in the topic will receive a verification SMS or email. You can delete mobile numbers and email addresses that do not need to receive verification messages.

Figure 5-6 SMS/Email



- **Verification code**

  Figure 5-7 Verification code



Step 3 Click **OK**. After 2FA is enabled, it takes about 5 minutes for the configuration to take effect.

NOTICE

When you log in to a remote Windows server from another Windows server where 2FA is enabled, you need to manually add credentials on the latter. Otherwise, the login will fail.

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

----End

6 Server Management

6.1 Creating a Server Group

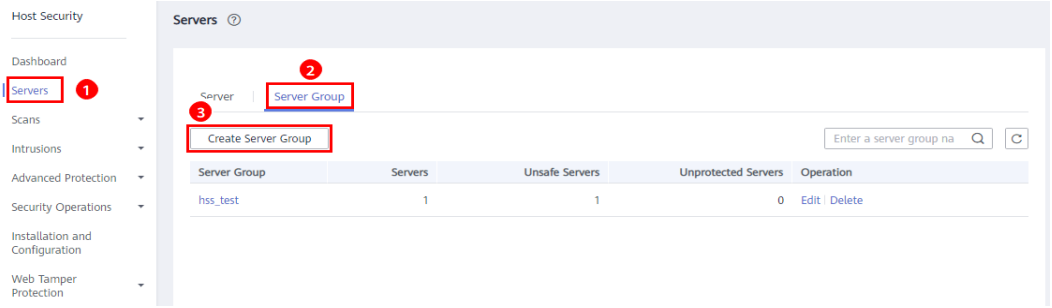
To manage servers by group, you can create a server group and add servers to it. You can check the numbers of servers, unsafe servers, and unprotected servers in a group.

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** > **Host Security Service**.

Step 3 In the navigation pane, choose **Servers**, and click the **Server Group** tab. Click **Create Server Group**, as shown in **Figure 6-1**.

Figure 6-1 Accessing the Server Group tab

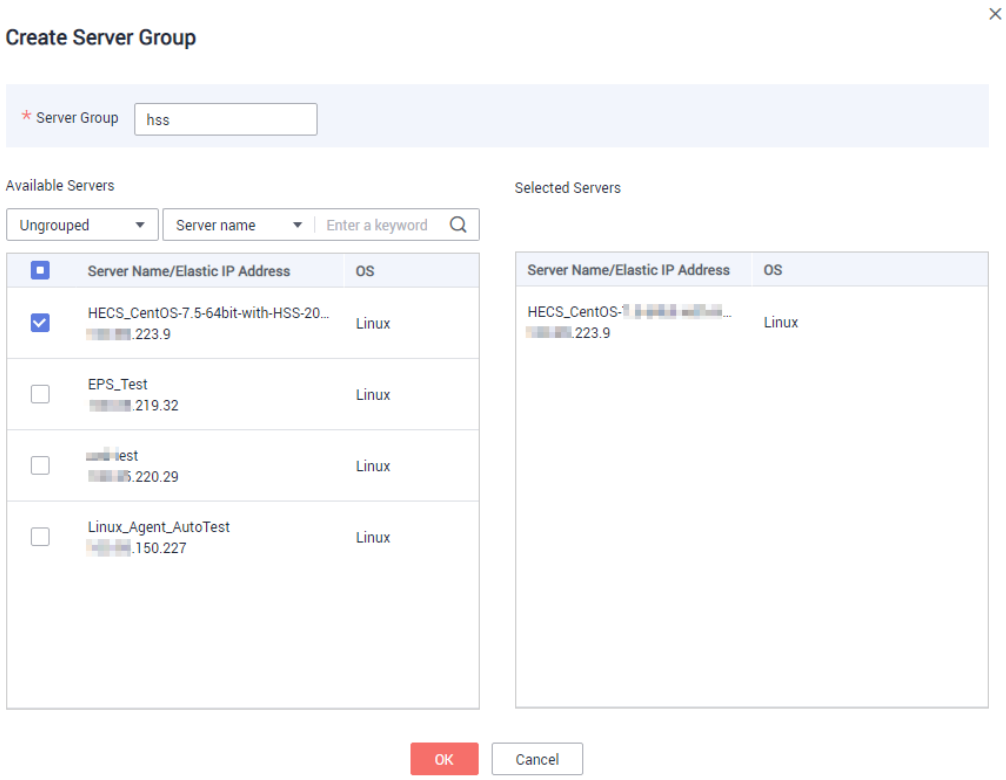


Step 4 In the **Create Server Group** dialog box, enter a server group name and select the servers to be added to the group, as shown in **Figure 6-2**.

NOTE

- The 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.

Figure 6-2 Creating a server group



Step 5 Click **OK**.

----End

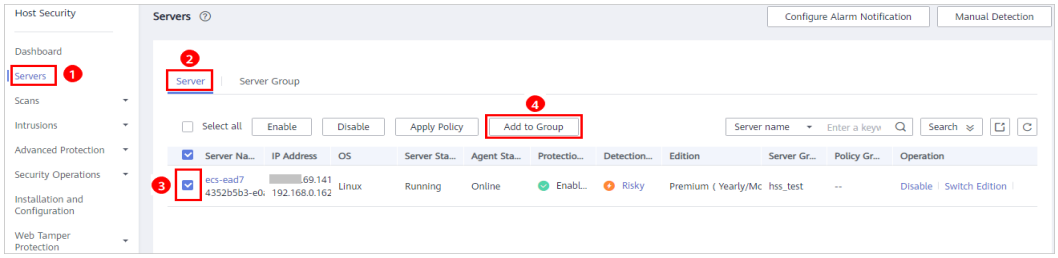
Adding Servers to Groups

You can add servers to an existing server group.

Step 1 Click the **Server** tab.

Step 2 Select one or more servers and click **Add to Group**, as shown in **Figure 6-3**.

Figure 6-3 Adding servers to a group



NOTE

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**.

Step 3 In the displayed dialog box, select a server group and click **OK**.

NOTE

A server can be added to only one server group.

----End

Follow-Up Procedure

Editing a server group

Step 1 Locate the row where a server group resides and click **Edit** in the **Operation** column.

Step 2 In the displayed dialog box, add or remove servers in the group.

Step 3 Click **OK**.

----End

Viewing a server group

In the server group list, click the name of a server group to view the server status, agent status, protection status, and scan results of servers the group.

Deleting a server group

Locate the row where a server group resides and click **Delete** in the **Operation** column.

After the server group is deleted, the **Server Group** column of the servers that were in the group will be blank.

6.2 Applying a 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 you enable the enterprise edition, the default policy group of this edition (including weak password and website shell detection policies) takes effect for all your servers.
- When you enable the premium or WTP edition, the edition is bound to **default_premium_policy_group**.

  To create your own policy group, you can copy the default policy group and add or remove policies in the copy.

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** > **Host Security Service**.

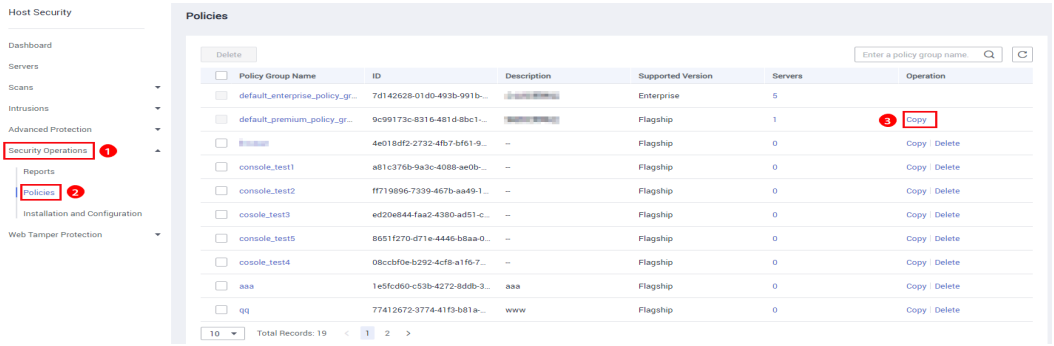
Step 3 In the navigation pane, choose **Security Operations** > **Policies**.

----End

Creating a Policy Group

Step 1 In the row where **default_premium_policy_group (default policy group of the premium edition)** resides, click **Copy** in the **Operation** column, as shown in **Figure 6-4**.

Figure 6-4 Copying a policy group

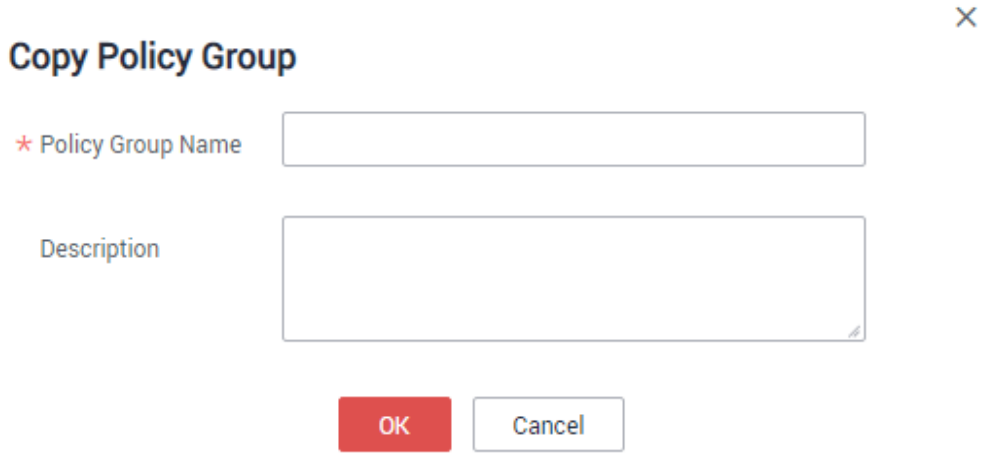


Step 2 In the dialog box displayed, enter a policy group name and description, and click **OK**, as shown in **Figure 6-5**.

NOTE

- 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.

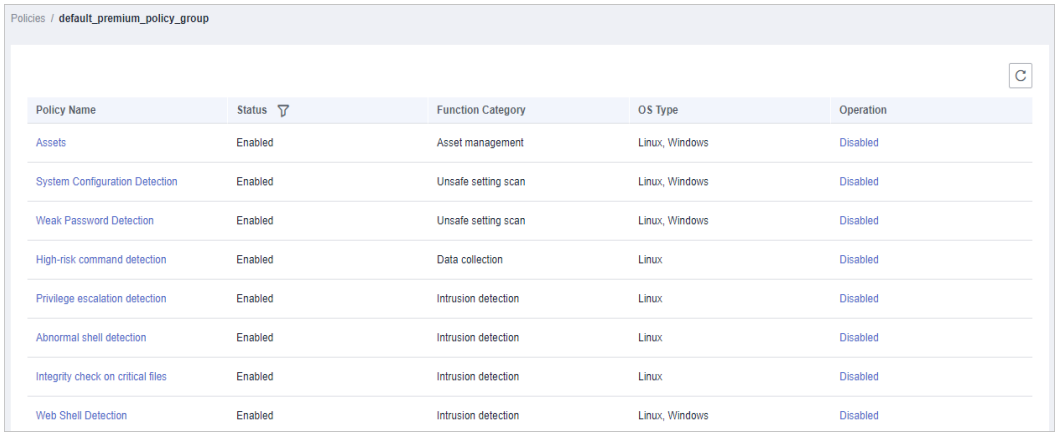
Figure 6-5 Creating a policy group



Step 3 Click **OK**.

Step 4 Click the name of the policy group you just created. The policies in the group will be displayed, as shown in **Figure 6-6**.

Figure 6-6 Policies in a group



Step 5 Click a policy name and modify its settings as required. For details, see **Modifying a Policy**.

Step 6 Enable or disable the policy by clicking the corresponding button in the **Operation** column.

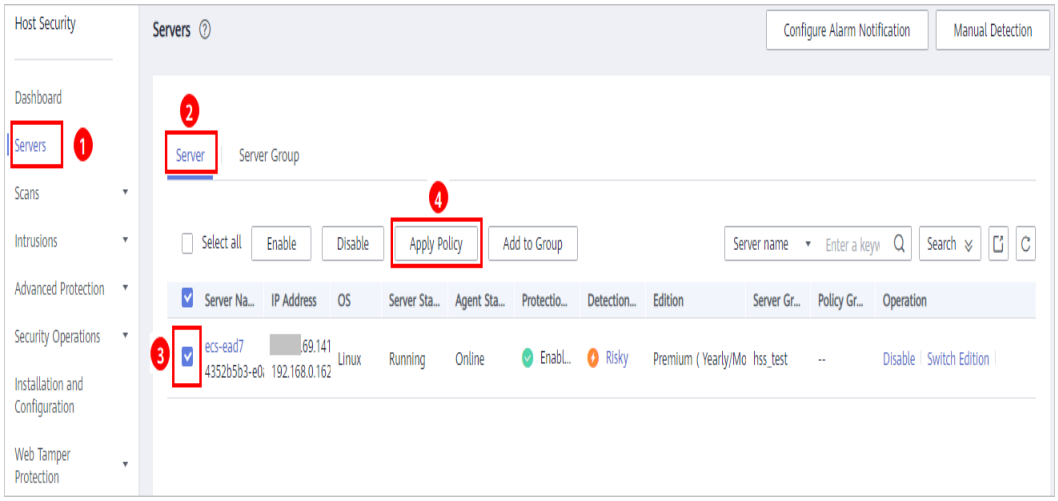
----End

Applying a Policy Group

Step 1 In the navigation pane, choose **Servers**. Click the **Server** tab.

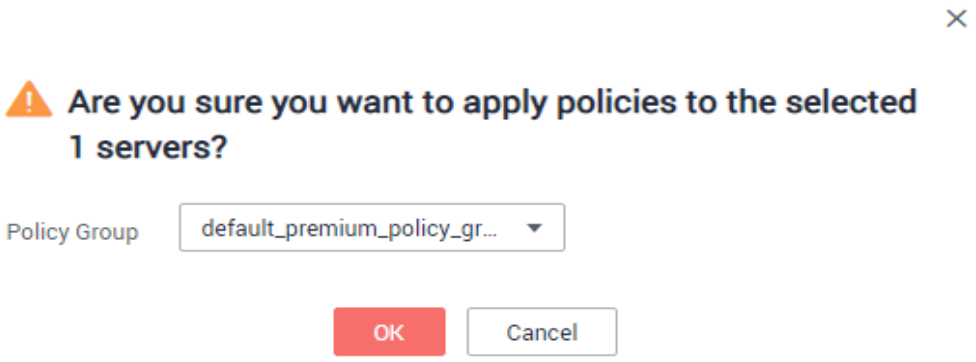
Step 2 Select one or more servers and click **Apply Policy**, as shown in **Figure 6-7**.

Figure 6-7 Applying policies



Step 3 In the dialog box that is displayed, select a policy group and click **OK**.

Figure 6-8 Selecting a policy group



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

7 Risk Prevention

7.1 Asset Management

HSS proactively checks open ports, processes, web directories, and auto-startup entries on your servers, and records changes on account and software information.

HSS lists all the assets on your servers and identifies risks in them in a timely manner.

HSS does not touch your assets. You need to manually eliminate the risks.

Check Interval

Account information and open ports are checked in real time.

Processes, web directories, software, and auto-start entries are checked in the early morning every day.

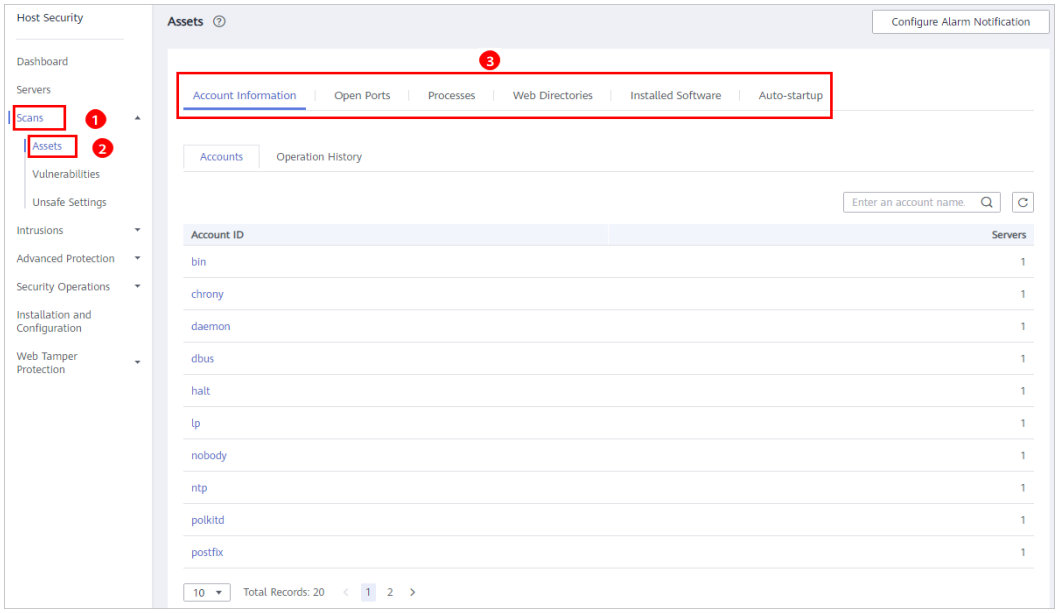
Viewing Asset Information

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** > **Host Security Service**.

Step 3 Go to the **Assets** page. Click tabs on the page to view assets detected by HSS on your servers.

Figure 7-1 Assets



----End

Managing Account Information

Operations made to accounts are recorded.

- The **Action** column records the operations. Its value can be **Create** (newly found in the latest check), **Delete** (found in earlier checks but missing in the latest check), and **Modify** (changes on account information, such as account names, administrator rights, and user groups, are detected).
- The **Time** column records the time when changes were detected, not the time when they were made.

You can check the information about and changes on all accounts here. If you find unnecessary or super-privileged accounts (such as **root**) that are not mandatory for services, delete them or modify their permissions to prevent exploits.

Checking Open Ports

You can manage all the open ports on your servers.

- 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.

Managing Processes

You can quickly check and terminate suspicious application processes on your servers.

If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.

Managing Web Directories

You can check and delete risky web directories and terminate suspicious processes in a timely manner.

Managing Software

Operations made to software are recorded.

- **Action**: **Create** and **Delete**.
- The **Time** column records the time when changes were detected, not the time when they were made.

You can check the information about and changes on all software, upgrade software, and delete software that is unnecessary, suspicious, or in old version.

Managing Auto-start Entries

Trojans usually intrude servers by creating auto-started services, scheduled tasks, preloaded dynamic libraries, run registry keys, or startup folders. The auto-startup check function collects information about all auto-started items, including their names, types, and number of affected servers, making it easy for you to locate suspicious auto-started items.

You can check the servers, paths, file hashes, and last modification time of auto-started items to find and eliminate Trojans in a timely manner.

7.2 Vulnerability Management

7.2.1 Viewing Details of a Vulnerability

HSS detects Linux software vulnerabilities, Windows system vulnerabilities, and Web-CMS vulnerabilities.

On the **Vulnerabilities** page, you can view the basic information and status about vulnerabilities and handle them based on **Urgency**.

In the chart of top 5 servers, only the vulnerabilities of **High** urgency are displayed.

Detection Mechanisms

Table 7-1 Vulnerability detection mechanisms

Type	Mechanism
Linux vulnerabilities	HSS detects vulnerabilities in the system and software (such as SSH, OpenSSL, Apache, and MySQL) based on vulnerability libraries, reports the results to the management console, and generates alarms.
Windows vulnerabilities	HSS subscribes to Microsoft official updates, 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.
Web-CMS vulnerabilities	HSS checks web directories and files for Web-CMS vulnerabilities, reports the results to the management console, and generates vulnerability alarms.

NOTE

Vulnerabilities detected in the past 24 hours are displayed. The server name in a vulnerability notification is the name used when the vulnerability was detected, and may be different from the latest server name.

Check Interval

HSS automatically performs a comprehensive check in the early morning every day.

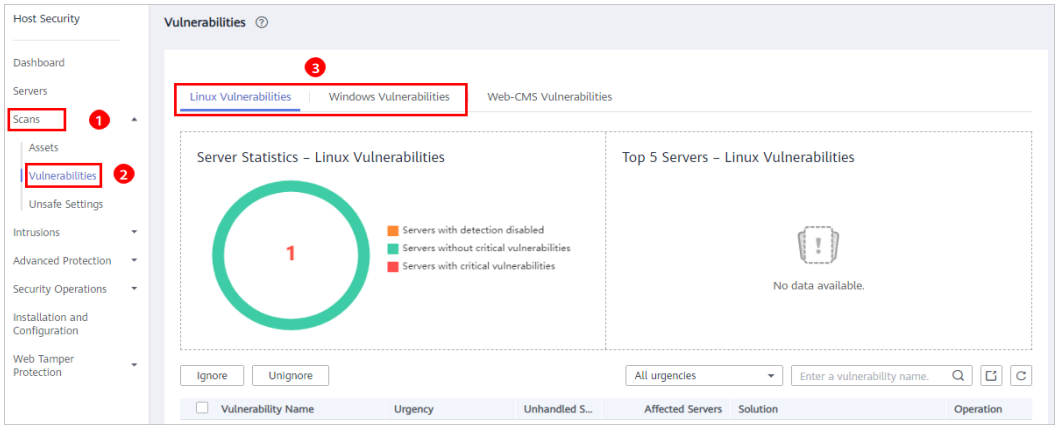
Fixing Linux or Windows Vulnerabilities

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** > **Host Security Service**.

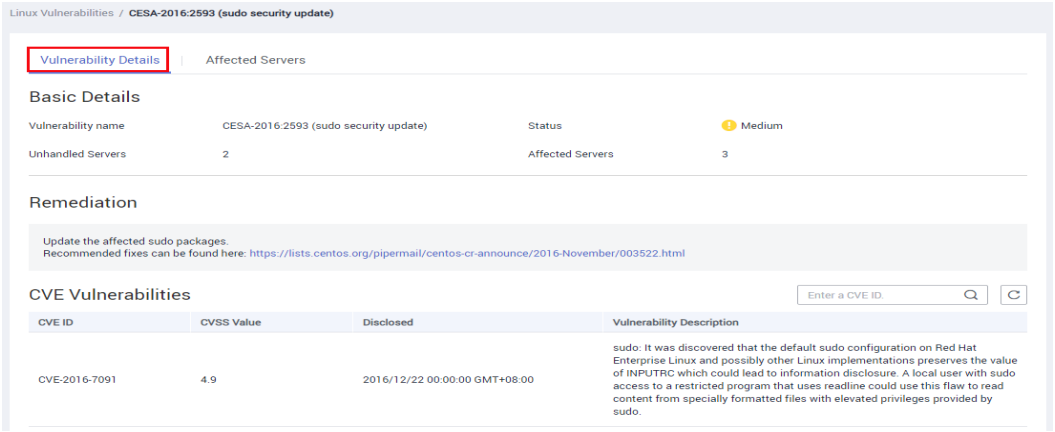
Step 3 Open the **Linux Vulnerabilities** or **Windows Vulnerabilities** tab.

Figure 7-2 Viewing Linux or Windows vulnerability scan results



Step 4 Click a vulnerability name to view its basic information, solution, and CVE description.

Figure 7-3 Checking vulnerability details



Step 5 Check the servers affected by the vulnerability.

Figure 7-4 Checking affected servers

- To fix the vulnerability, click **Fix**.
- To ignore the vulnerability, click **Ignore**. HSS will no longer generate alarms for this vulnerability.
- After the vulnerability is fixed, you can click **Verify** to verify the fix.

  HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.

  If a vulnerability fails to be rectified, click **View Cause** to check the details.

----End

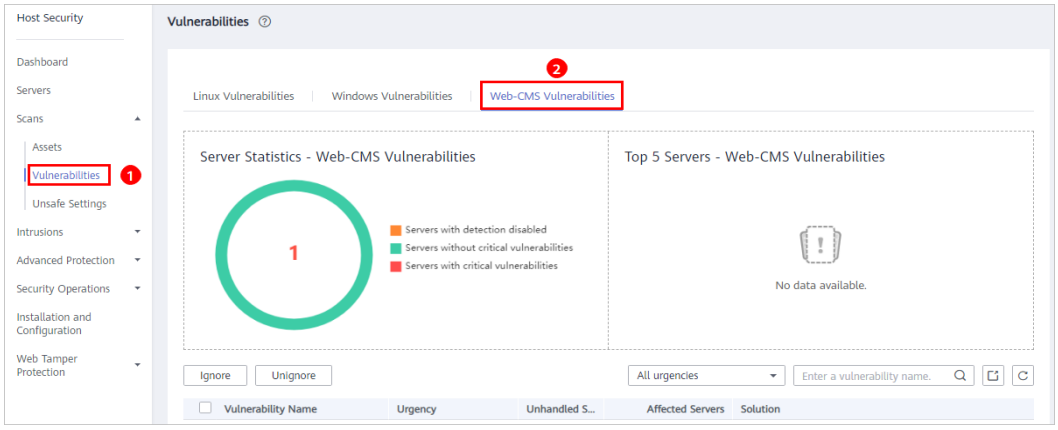
Fixing Web-CMS Vulnerabilities

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** > **Host Security Service**.

Step 3 Open the **Web-CMS Vulnerabilities** tab.

Figure 7-5 Viewing Web-CMS vulnerability detection results



Step 4 Click the vulnerability name to view its details and affected servers.

- No **Fix** options are provided in the **Operation** column. You need to manually fix the vulnerabilities based on the suggestions provided.
- After the vulnerability is fixed, manually verify the result. HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.
- To ignore the vulnerability, click **Ignore**. HSS will no longer generate alarms for this vulnerability.

Figure 7-6 Vulnerability details

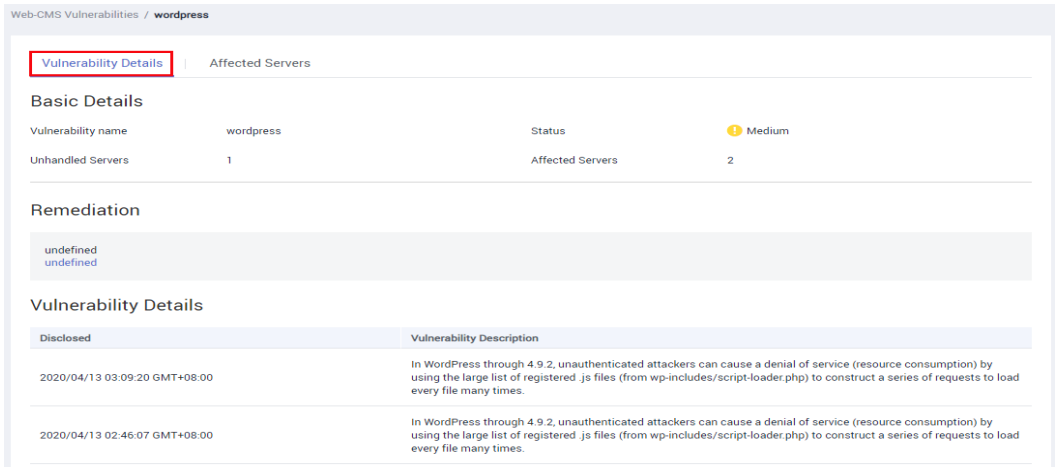
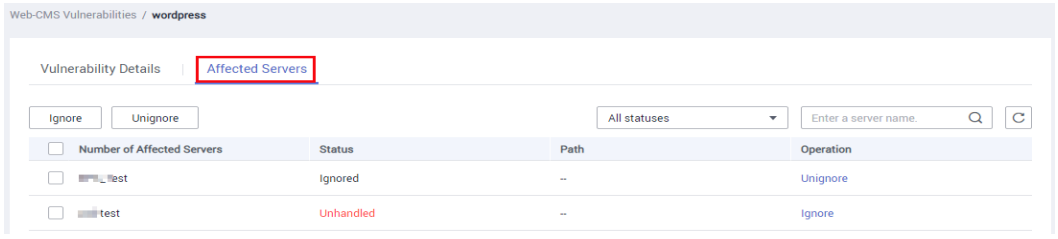


Figure 7-7 Affected servers



----End

Exporting a Vulnerability Report

In the upper right corner of the vulnerability list, click  to export the vulnerability report.

7.2.2 Fixing Vulnerabilities and Verifying the Result

- Linux or Windows vulnerabilities

  You can select servers and click **Fix** to let HSS fix the vulnerabilities for you, or manually fix them based on the suggestions provided.

  Then, you can use the verification function to quickly check whether the vulnerability has been fixed.

  NOTICE

  To fix Windows vulnerabilities, you need to connect to the Internet.

- Web-CMS vulnerabilities

  Manually fix them based on the suggestions provided on the page.

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 avoid unrecoverable errors, you are advised to use Cloud Server Backup Service (CSBS) to back up your servers. 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.

Urgency

- **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.
- **Safe for now**: This vulnerability has a small threat to server security. You can choose to fix or ignore it.

Vulnerability Display

- Vulnerabilities that failed to be fixed or have not been handled are always displayed in the vulnerability list.
- Fixed vulnerabilities will remain in the list within 30 days after it was fixed.

Fixing Vulnerabilities in One Click

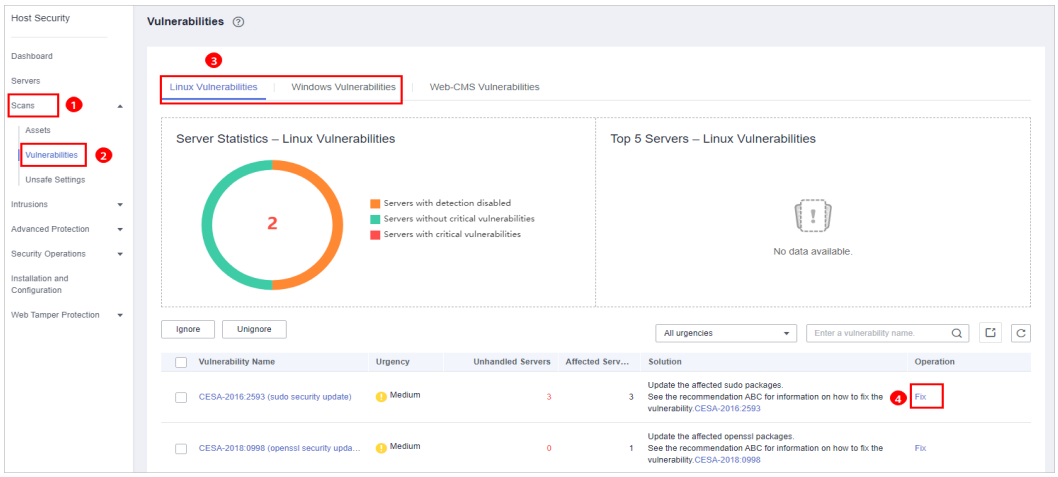
You can fix vulnerabilities in Linux or Windows OS in one click on the console.

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** > **Host Security Service**.

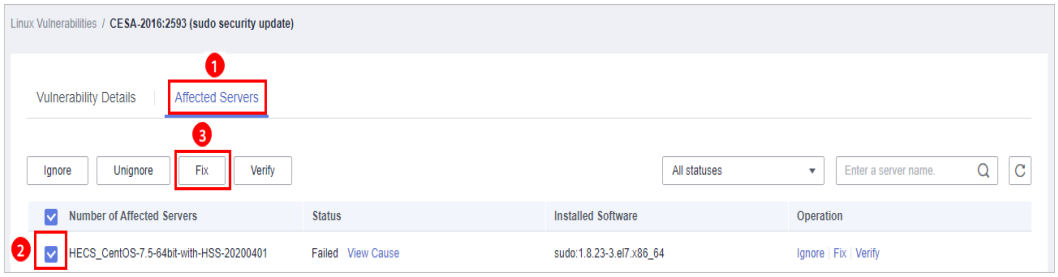
Step 3 On the **Vulnerabilities** page, click **Fix**. The **Affected Servers** tab is displayed, as shown in **Figure 7-8**.

Figure 7-8 Fixing vulnerabilities



Step 4 Select the affected servers and click **Fix**.

Figure 7-9 One-click vulnerability fix



Step 5 In the dialog box that is 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.**

Step 6 Click **OK** to fix the vulnerability in one-click mode. The vulnerability status will change to **Fixing**.

If a vulnerability is fixed, its status will change to **Repaired**. If it fails to be fixed, its status will change to **Failed**.

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.

----End

Manually Fixing Software Vulnerabilities

Fix the detected vulnerability based on the fix suggestions in the **Solution** column. For details about the vulnerability fix commands, see **Table 7-2**.

- 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.

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 7-2 Vulnerability fix commands

OS	Command
CentOS/Fedora/EulerOS/Red Hat/Oracle	yum update Software name
Debian/Ubuntu	apt-get update && apt-get install Software name --only-upgrade
Gentoo/SUSE	See the vulnerability fix suggestions for details.

Vulnerability fixing may affect service stability. You are advised to use either of the following methods to avoid such impact:

Method 1: Create a VM to fix the vulnerability.

1. Create an image for the ECS to be fixed.
2. Use the image to create an ECS.
3. Fix the vulnerability on the new ECS and verify the result.
4. Switch services over to the new ECS and verify they are stably running.
5. Release the original ECS. If a fault occurs after the service switchover and cannot be rectified, you can switch services back to the original ECS.

Method 2: Fix the vulnerability on the target server.

1. Create a backup for the ECS to be fixed.
2. Fix vulnerabilities on the current server.
3. If services become unavailable after the vulnerability is fixed and cannot be recovered in a timely manner, use the backup to restore the server.

NOTE

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

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. Such vulnerabilities can be ignored.

HSS will not generate alarms for ignored vulnerabilities.

Verifying Vulnerability Fix

After a vulnerability is fixed, you are advised to verify it immediately.

Manual verification

- Click **Verify** on the vulnerability details page.
- Ensure the software has been upgraded to the latest version. The following table provides the commands to check the software upgrade result.

  Table 7-3 Verification commands

OS	Verification Command
CentOS/Fedora/ EulerOS/Red Hat/Oracle	rpm -qa | grep *Software_name*
Debian/Ubuntu	dpkg -l | grep *Software_name*
Gentoo	emerge --search *Software_name*
SUSE	zypper search -dC --match-words *Software_name*

- Manually check for vulnerabilities and view the vulnerability fixing results.

Automatic verification

HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.

7.3 Baseline Inspection

7.3.1 Checking for Unsafe Settings

HSS checks your software for weak password complexity policies and other unsafe settings, and provides **suggestions** for fixing detected risks.

Check Interval

- HSS automatically performs a comprehensive check in the early morning every day.
- To manually start a scan, click **Manual Detection** in the upper right corner of the **Servers** page.

HSS will scan your servers for software information, Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, web shells, password risks, and unsafe settings configuration.

All these items are concurrently checked and the total scan duration is less than 30 minutes.

- To view the scan details of a server, click its scan result in the **Detection Result** column on the **Servers and Quotas** page.

  You can also scan for password risks or unsafe configurations alone. On the **Unsafe Settings** tab of the result page, click the **Password Risks** or **Unsafe Configurations** subtab and click **Manual Detection**. The scan takes less than 30 minutes.

Alarm Policies

HSS checks your servers for weak passwords and unsafe software settings, and generates alarms if it finds any of them.

NOTE

You can enable alarm notifications on the **Installation and Configuration** page of the HSS console. For details, see **Enabling Alarm Notification for the Basic/Enterprise/Premium Edition**.

Check Items

Table 7-4 Check items

Item	Description
Password complexity policies	Password complexity policies on system accounts
Common weak passwords	Weak passwords defined in the common weak password library Common weak passwords of MySQL, FTP, and system accounts
Unsafe configurations	Unsafe configurations in Tomcat, SSH, Nginx, Redis, Apache2, and MySQL5

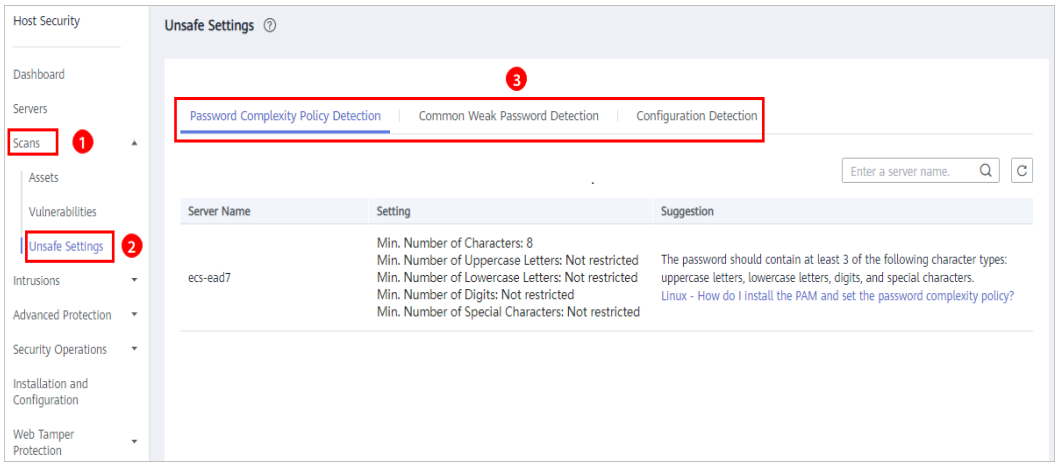
Procedure

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** > **Host Security Service**.

Step 3 Choose **Scans** > **Unsafe Settings** and check detected unsafe settings.

Figure 7-10 Unsafe settings



----End

Exporting a Check Report

On the upper right corner of the table on the **Configuration Detection** tab, click  to download reports.

NOTE

The detection result of a single server cannot be separately exported.

7.3.2 Suggestions on Fixing Unsafe Settings

This topic provides suggestions on how to fix unsafe settings found by HSS.

Modifying 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?**

After modifying the password complexity policy, you are advised to perform manual detection immediately to verify the result. If you do not perform manual verification, HSS will automatically check the settings the next day in the early morning.

Weak Passwords

- To enhance server security, you are advised to modify the accounts with weak passwords for logging in to the system 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.

After modifying weak passwords, you are advised to perform manual detection immediately to verify the result. If you do not perform manual verification, HSS will automatically check the settings the next day in the early morning.

Unsafe Configurations

Insecure configurations of key applications will probably be exploited by hackers to intrude servers. Such configurations include insecure encryption algorithms used by SSH and Tomcat startup with root permissions.

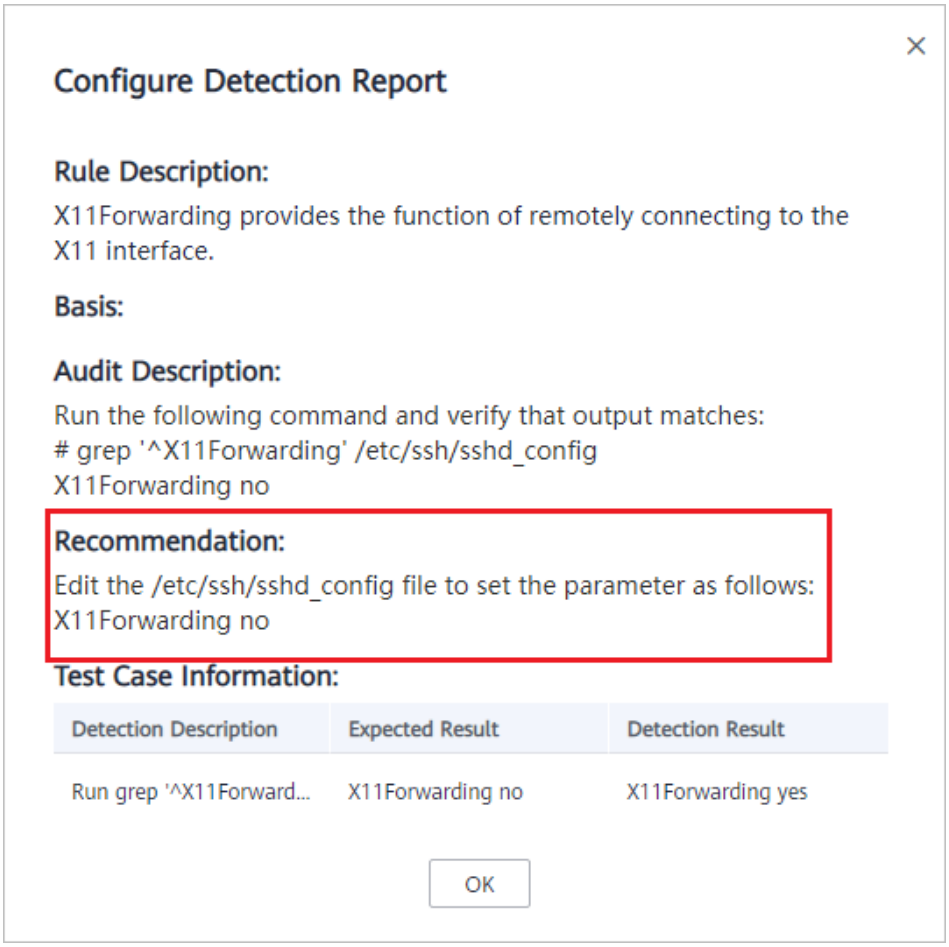
HSS can detect unsafe configurations provide detailed suggestions. You can check, fix, or ignore a risky item.

- Modifying unsafe configuration items

  You can confirm the detection result based on details under **Audit Description** and fix settings as instructed in **Recommendation**.

  You are advised to fix the configurations with high severity immediately and repair those with medium or low severity based on service requirements.

  Figure 7-11 Detection report



- Ignoring trusted configuration items

  Select a detection rule and click **Ignore** in the **Operation** column to ignore it. To ignore multiple detection rules, select them and click the **Ignore** button above the list to batch ignore them.

  To unignore an ignored detection rule, click **Unignore** in the **Operation** column. To unignore multiple ignored detection rules, select rules and click **Unignore** in the upper left corner above the detection rule list.

After modifying configuration items, you are advised to perform manual detection immediately to verify the result. If you do not perform manual verification, HSS will automatically check the settings the next day in the early morning.

8 Intrusion Detection

8.1 Alarm Events

HSS generates alarms on 13 types of intrusion events, including brute-force attacks, abnormal process behavior, web shells, abnormal logins, and malicious processes. You can learn all these events on the HSS console and eliminates security risks in your assets in a timely manner.

Alarm Events

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Brute-force attack	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. Detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts. ● If the number of brute-force attacks from an IP address reaches 5 within 30 seconds, the IP address will be blocked. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. ● You can check whether the 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.	√	√	√	√
Abnormal login	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 you set, an alarm will be triggered. ● Trigger an alarm if a user logs in by a brute-force attack.	√	√	√	√

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Malicious program (cloud scan)	Malicious programs include 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. 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.	×	√ (Isolate and kill)	√ (Isolate and kill)	√ (Isolate and kill)
Abnormal process behavior	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 CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections	×	√	√	√

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Critical file change	If hackers intrude into your system, they will probably tamper with important system files to forge identities or prepare for further attacks. • Check alarms about modifications on key files (such as **ls**, **ps**, **login**, and **top**). For details about the monitored paths, see **Monitored Important File Paths**. • Key file change information includes the paths of modified files, the last modification time, and names of the servers storing configuration files. • You can add fingerprint libraries of critical files, so that HSS can better collect critical file information and detect exceptions. HSS only checks whether directories or files have been modified, not whether they are modified manually or by a process.	×	√	√	√
Web shell	A web shell is a command execution environment in the form of web page files, such as PHP and JSP files. After hacking a website, a hacker usually puts a web shell among normal web page files in the web directory of a website server, and then accesses the web shell through a browser to control the server. Check whether the files (often PHP and JSP files) 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.	×	√	√	√

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Reverse shell	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. You can configure the reverse shell detection rule on the **Policies** page. HSS will check for suspicious or remotely executed commands.	×	×	√	√
Abnormal shell	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 reverse shell detection rule on the **Policies** page. HSS will check for suspicious or remotely executed commands.	×	×	√	√
High-risk command execution	You can configure what commands will trigger alarms in the **High-risk command detection** rule on the **Policies** page. HSS checks executed commands in real time and generates alarms if high-risk commands are detected.	×	×	√	√
Auto-startup check	Trojans usually intrude servers by creating auto-started services, scheduled tasks, or preloaded dynamic libraries. The auto-startup check function collects information about all auto-started items, including their names, types, and number of affected servers. HSS checks and lists auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders.	×	×	√	√
Unsafe account	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.	×	√	√	√

Alarm Name	Description	Basic	Enterprise	Premium	WTP
Privilege escalation	After hackers intrude servers, 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 detects privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: ● Root privilege escalation by exploiting SUID program vulnerabilities ● Root privilege escalation by exploiting kernel vulnerabilities ● File privilege escalation	×	×	√	√
Rootkit	HSS detects suspicious rootkit installation in a timely manner by checking: ● Rootkits based on file signatures ● Hidden files, ports, and processes	×	×	√	√

Monitored Important File Paths

Type	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/netstat /bin/login /bin/find /bin/lsmod /bin/pidof /bin/lsof /bin/ss

Type	Linux
usr	/usr/bin/ls /usr/bin/ps /usr/sbin/ps /usr/bin/bash /usr/bin/netstat /usr/sbin/netstat /usr/sbin/rsyslogd /usr/sbin/ifconfig /usr/bin/login /usr/bin/find /usr/sbin/lsmod /usr/sbin/pidof /usr/bin/lsof /usr/sbin/lsof /usr/sbin/tcpd /usr/bin/passwd /usr/bin/top /usr/bin/du /usr/bin/chfn /usr/bin/chsh /usr/bin/killall /usr/bin/ss /usr/sbin/ss /usr/bin/ssh /usr/bin/scp
sbin	/sbin/syslog-ng /sbin/rsyslogd /sbin/ifconfig /sbin/lsmod /sbin/pidof

8.2 Checking and Handling Intrusion Events

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 servers with alarms, handled alarms, unhandled alarms, blocked IP addresses, and isolated files.

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 and Limitations

- To skip the checks on high-risk command execution, privilege escalation, 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.
- Other detection items cannot be manually disabled.

Checking Alarm 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** > **Host Security Service**.

Step 3 In the navigation pane, choose **Intrusions** > **Events**, as shown in **Figure 8-1**.

Figure 8-1 Events page

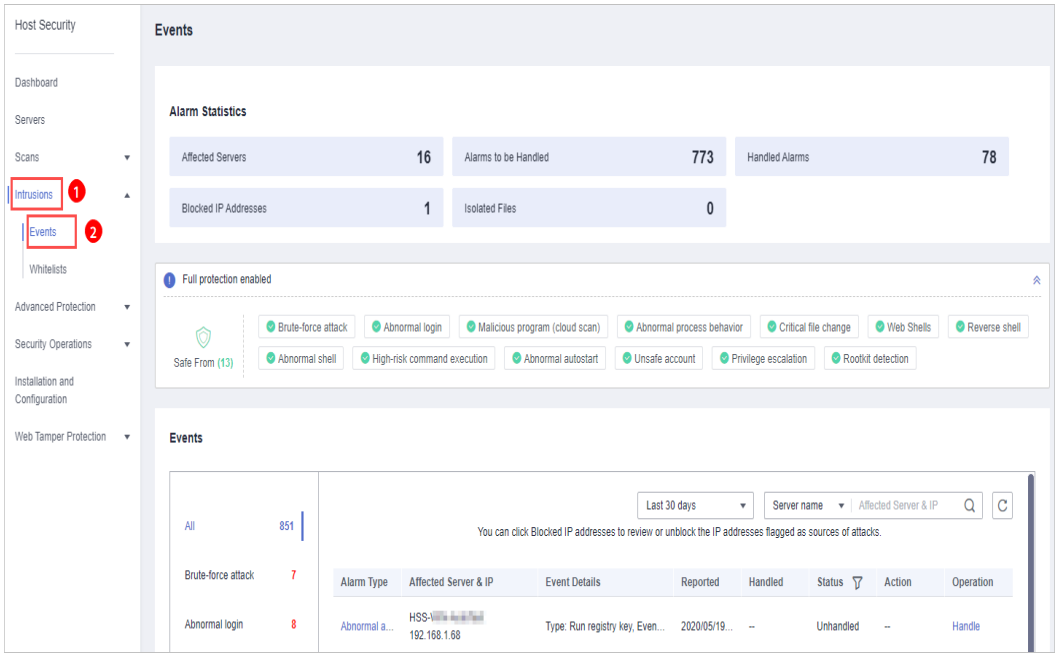


Table 8-1 Alarm events

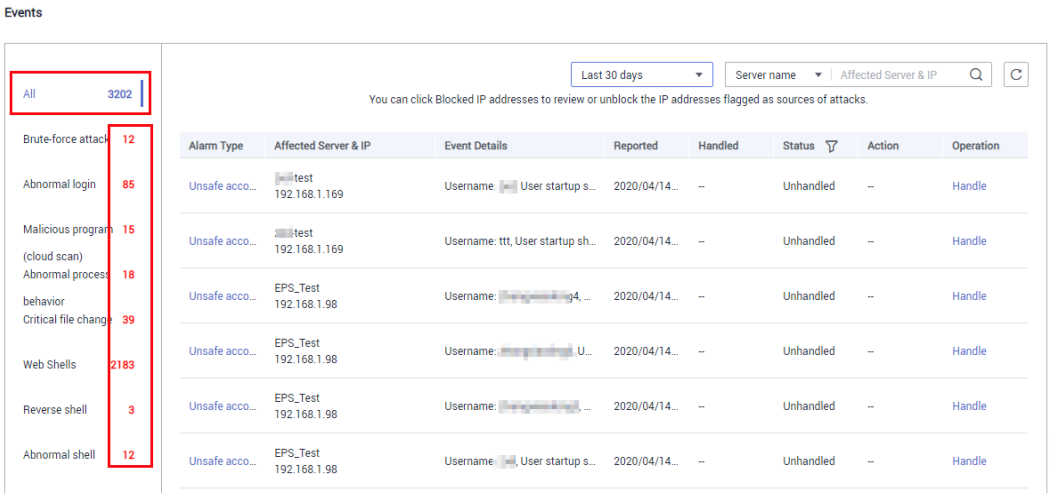
Alarm Event	Description
Affected Servers	Number of servers for which alarms are generated.
Alarms to be Handled	Number of alarms to be handled. By default, all unhandled alarms are displayed on the **Events** page. For more information, see **Handling Alarm Events**.

Alarm Event	Description
Handled Alarms	Number of handled alarms.
Blocked IP Addresses	Number of blocked IP addresses. You can click the number to check blocked IP address list. 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. **NOTICE** After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address.
Isolated Files	HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Events** 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**.

Step 4 Click an alarm event in the list to view the affected servers and occurrence time of the event, as shown in **Figure 8-2**. The following information is displayed:

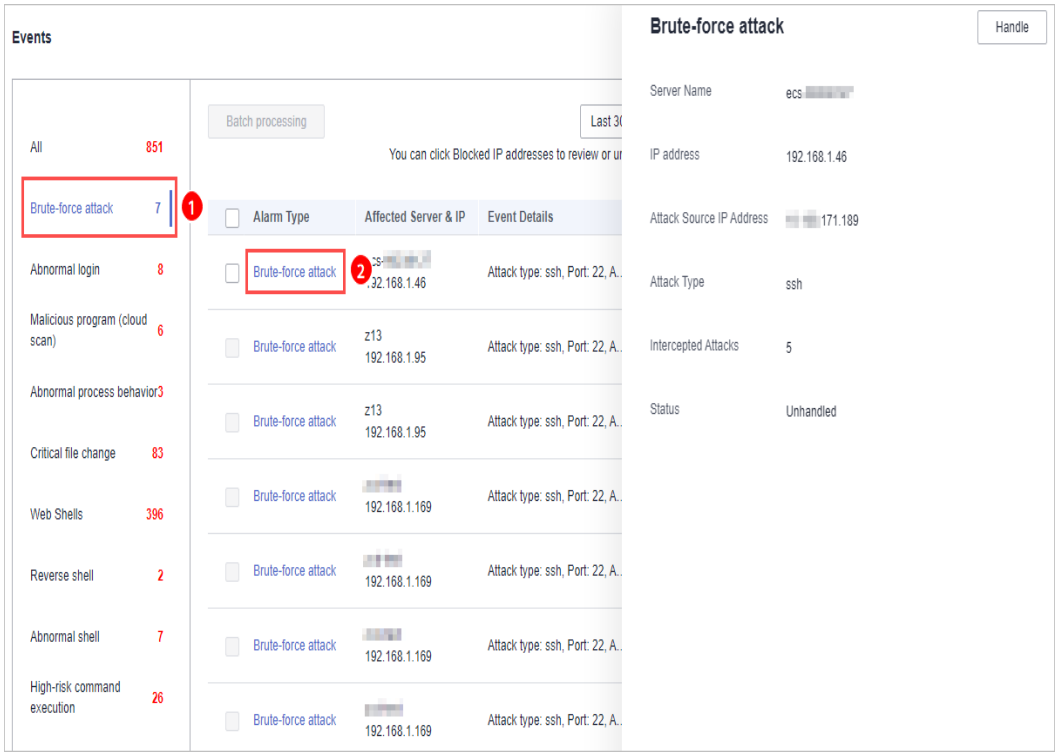
- Total number of alarms
- Number of each type of alarms

Figure 8-2 Alarm event statistics



Step 5 Click an alarm name to view its details, as shown in **Figure 8-3**.

Figure 8-3 Alarm details



----End

Handling Alarm Events

This section describes how you should handle alarm events to ensure server security.

NOTE

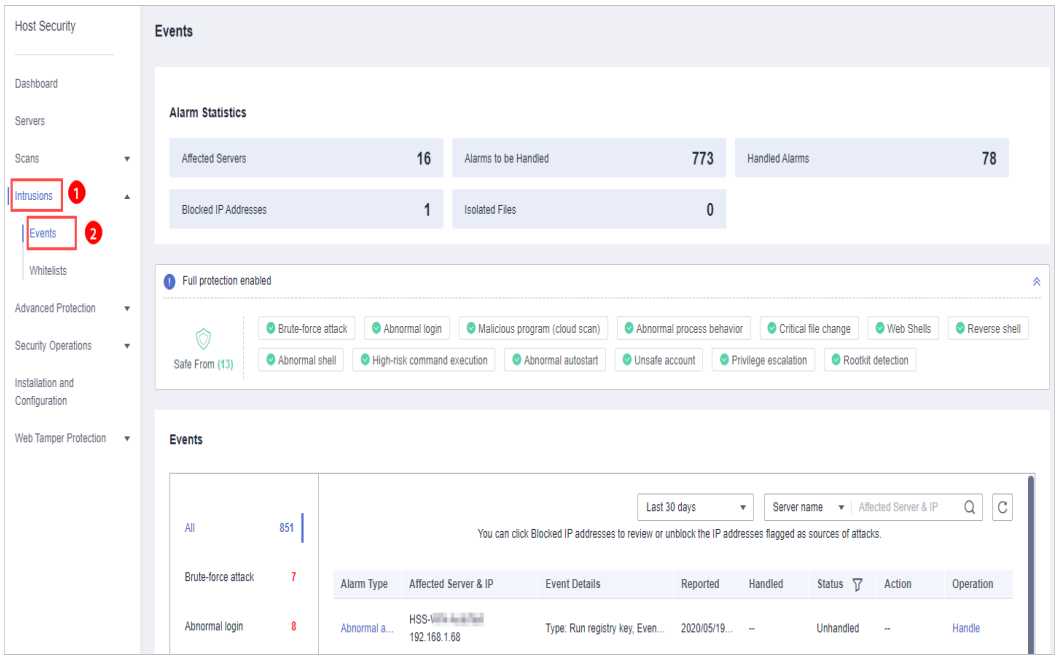
Do not fully rely on alarms to defend against attacks, because not every issue can be detected in a timely manner. You are advised to take more measures to prevent threats, such as checking for and fixing vulnerabilities and unsafe settings.

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** > **Host Security Service**.

Step 3 In the navigation pane, choose **Intrusions** > **Events**.

Figure 8-4 Events page

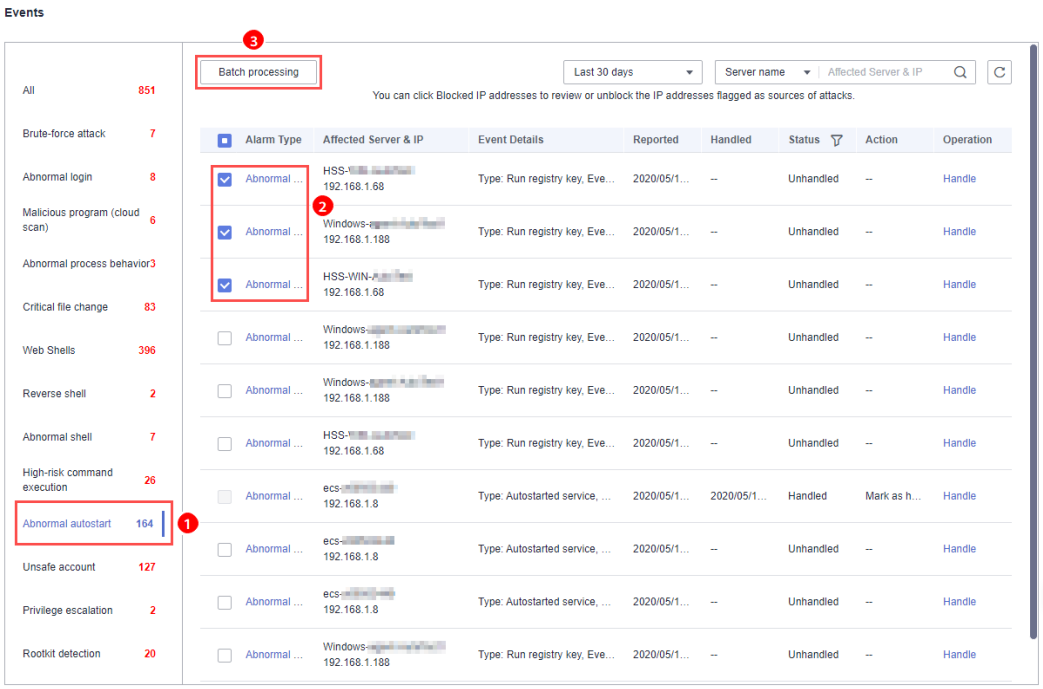


Step 4 Click an event type, select events, and click **Handle**, as shown in **Figure 8-5**. **Table 8-2** describes the processing methods you can choose from.

NOTE

You can also click **Handle** in the row where an alarm resides.

Figure 8-5 Handling alarm events



Alarm events are displayed on the **Events** page. Here you can check up to 30 days of historical events.

Check and handle alarm events as needed. The status of a handled event changes from **Unhandled** to **Handled**. HSS will no longer collect its statistics or display them on the **Dashboard** page.

Table 8-2 Event handling methods

Method	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**. The following types of alarm events support online isolation and killing: • Malicious program (cloud scan) • Abnormal process behavior **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).
Mark as handled	Mark the event as handled. You can add remarks for the event to record more details.
Add to 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 whitelisted items.
Add to alarm whitelist	Add false alarmed items of the following types to the login whitelist. HSS will no longer report alarm on the whitelisted items. • Reverse shell • Web shell • Abnormal process behavior • Process privilege escalation • File privilege escalation • High-risk command • Malicious program

----End

Handling Suggestion

Alarm Name	Suggestion
Brute-force attack	**Pay special attention to such events.** If you receive a brute-force attack alarm, detected events will probably be but are not limited to: ● The system uses weak passwords and is under brute-force attacks. ● Attackers correctly guess the password and log in after several failed attempts (before their login IP addresses are blocked). You are advised to check whether the alarmed login IP address is valid. ● If the source IP address is valid, ignore the alarms and manually unblock the IP addresses.Alternatively, whitelist the alarmed IP address. This IP address will no longer trigger alarms. ● If the source login IP address are unknown, your servers may have been intruded by hackers. 1. You are advised to mark the event as **Handled**. 2. Immediately log in to the intruded account and set a strong password. 3. Check all the accounts and delete suspicious accounts to prevent attackers from creating new accounts or changing account permissions. 4. Check for malicious programs on servers. Then, log in to the servers where the malicious programs are running and stop them immediately.
Abnormal login	If an abnormal login is detected, you are advised to immediately check whether the source IP address is valid. ● If it is valid, you can ignore this event. If the login location is valid, you can add the location to the list of common login locations. ● If it is invalid or unknown, your servers have been intruded. In this case, you are advised to mark the event as **Handled**, immediately change the account password, and scan the entire system for risks to prevent further damage.

Alarm Name	Suggestion
Malicious program (cloud scan)	Common methods to handle the event are as follows: ● If the programs are normal, ignore the event or whitelist the program. The programs will no longer trigger such events. ● If the programs are unknown or malicious, you are advised to immediately kill them and isolate their source files. – You can isolate and kill detected or suspicious programs in one click. Alternatively, you can mark the event as **Handled**, immediately log in and stop the program, and scan the entire system for risks to prevent further damage. – HSS can isolate and kill malicious programs, including common ransomware, DDoS viruses, and Trojans. You are advised to enable this function to harden server security. ● If the programs are harmless or mandatory for service operation, you can cancel isolation and restore the program source files.
Abnormal process behavior	If abnormal process behaviors are detected, you are advised to check processes immediately. ● If the processes are normal, ignore the event or whitelist the process. The processes will no longer trigger such events. ● If the processes are unknown or malicious, you are advised to immediately kill them and isolate their source files. – You can isolate and kill detected or suspicious programs in one click. Alternatively, you can mark the event as **Handled**, immediately log in and stop the program, and scan the entire system for risks to prevent further damage. – HSS can isolate and kill malicious programs, including common ransomware, DDoS viruses, and Trojans. You are advised to enable this function to harden server security. ● If the programs are harmless or mandatory for service operation, you can cancel isolation and restore the program source files.
Critical file change	If a key file change is detected, you are advised to check the change immediately. ● If the change is valid, you can ignore the event. ● If the change is invalid, critical files have been read, written, or deleted without authorization. You are advised to mark the event has **Handled** and immediately replace the file with the standard version of the OS. Log in to intruded accounts and change their passwords, and scan the entire system for risks to prevent further damage.

Alarm Name	Suggestion
Web shell	If a web shell is detected, you are advised to immediately check whether the file is valid. ● If the file is valid, ignore the event or whitelist the file. The file will no longer trigger such events. ● If the file is invalid, you are advised to mark the event as **Handled** and immediately isolate the file.
Reverse/ Abnormal shell	If a reverse or abnormal shell is detected, you are advised to check whether executed commands are valid. ● If they are valid, you can ignore this event. ● If they are invalid, mark the event as **Handled** and immediately log in to the system to block invalid connections or stop command execution, and scan the entire system for risks to prevent further damage.
High-risk command execution	If a high-risk command is detected, you are advised to immediately check whether the command is valid. ● If it is valid, ignore the event or whitelist the command. The command will no longer trigger such events. ● If it is invalid, mark the event as **Handled** and immediately log in to the system and check operations performed using the command, and scan the entire system for risks to prevent further damage.
Auto-startup check	If a new auto-started item is detected, you need to check whether the auto-startup item is valid. ● If it is valid, ignore the event or whitelist the command. The command will no longer trigger such events. ● If it is invalid, mark the event as **Handled** and immediately log in to the system to delete the item, and scan the entire system for risks to prevent further damage.
Unsafe account	If an unsafe account is detected, you are advised to immediately check whether the account is valid. ● If it is valid, you can ignore this event. ● If it is invalid, mark the event as a **Handled** and perform the following operations: – Deleting suspicious accounts Delete unnecessary system login accounts, such as SSH accounts, from the servers. Delete unnecessary accounts used by the MySQL and FTP services from the servers. – Limiting account permissions Specify key configuration items to limit the file access and modification permissions of non-administrators, preventing unauthorized access and operations.

Alarm Name	Suggestion
Privilege escalation	If a privilege escalation operation is detected, you are advised to immediately check whether the operation is valid. • If it is valid, you can ignore this event. • If it is invalid, mark the event as **Handled** and immediately log in to the system to block invalid connections or stop command execution, and scan the entire system for risks to prevent further damage.
Rootkit	If Rootkit installation is detected, you are advised to immediately check whether the installation is valid. • If it is valid, you can ignore this event. • If it is invalid, mark the event as **Handled** and immediately log in to the system to stop Rootkit installation, and scan the entire system for risks to prevent further damage.

8.3 Managing Isolated Files

HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Events** page and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check them, You can isolate files or recover them.

The following types of alarm events support online isolation and killing:

- Malicious program (cloud scan)
- Abnormal process behavior

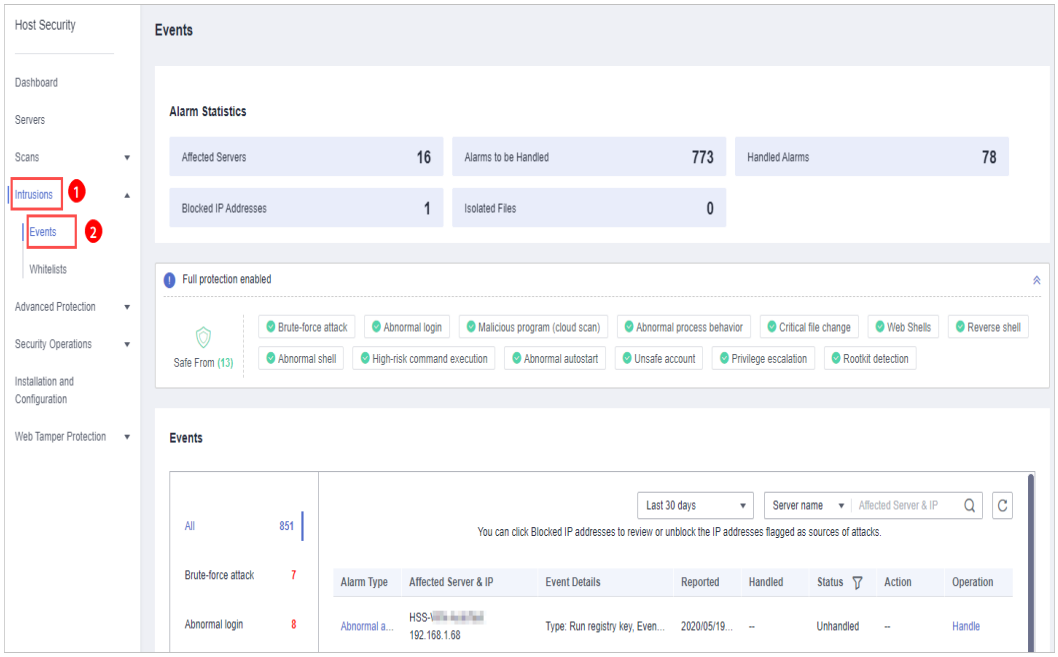
Isolating and Killing Files

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** > **Host Security Service**.

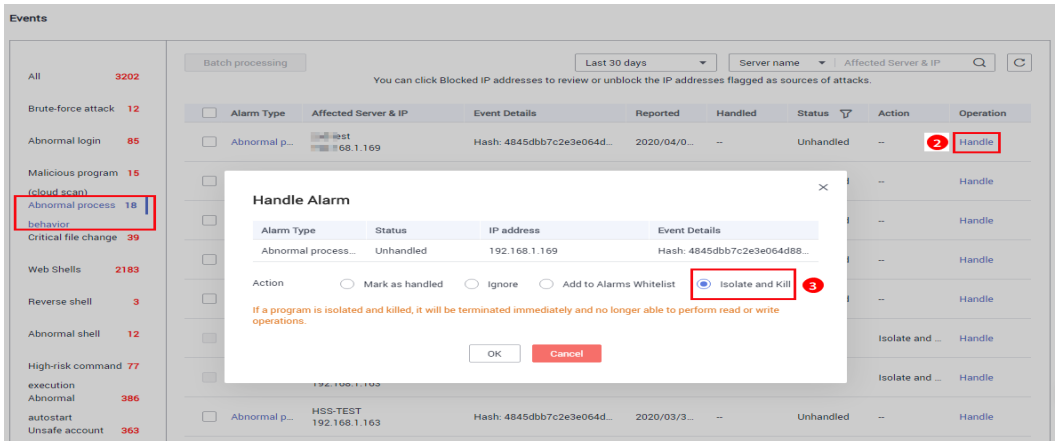
Step 3 In the navigation pane, choose **Intrusions** > **Events**.

Figure 8-6 Events page



Step 4 Select an event of the **Malicious program (cloud scan)** or **Abnormal process behavior** type, and click **Handle**. In the dialog box that is displayed, click **Isolate and Kill**.

Figure 8-7 Isolating and killing malicious programs



Step 5 Click **OK**. Files that have been isolated are displayed on a slide-out panel on the Events page and cannot harm your servers. You can click **Isolated Files** on the upper right corner to check them.

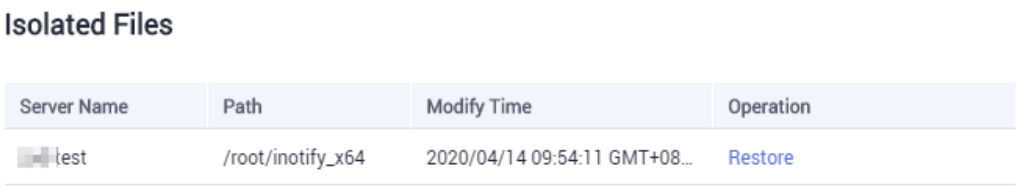
----End

Checking Isolated Files

Step 1 On the **Events** page, click **Isolated Files** on the upper right corner.

Step 2 Check the servers, names, paths, and modification time of the isolated files, as shown in **Figure 8-8**.

Figure 8-8 Checking isolated files



----End

Recovering Isolated Files

Step 1 Click **Restore** in the **Operation** column of an isolated file.

Step 2 Click **OK**.

NOTE

Recovered files will no longer be isolated. Exercise caution when performing this operation.

----End

8.4 Configuring the Alarm Whitelist

You can configure the alarm whitelist to reduce false alarms. Events can be batch imported to and exported from the whitelist.

Whitelisted events will not trigger alarms.

On the **Events** page, you can add falsely reported alarms to the alarm whitelist. HSS will no longer generate alarms for it, and its statistics will not be displayed on the **Dashboard** page.

Adding Events to the Alarm Whitelist

Table 8-3 Configuring the alarm whitelist

Method	Description
Add to alarm whitelist	Choose to add the alarm to the whitelist when handling it. For details, see **Checking and Handling Intrusion Events**. The following types of events can be added to the alarm whitelist: • Reverse shell • Web shell • Abnormal process behavior • Process privilege escalation • File privilege escalation • High-risk command • Malicious program
Import the alarm whitelist	You can import whitelisted items on the **Alarm Whitelist** tab.

Checking the Alarm Whitelist

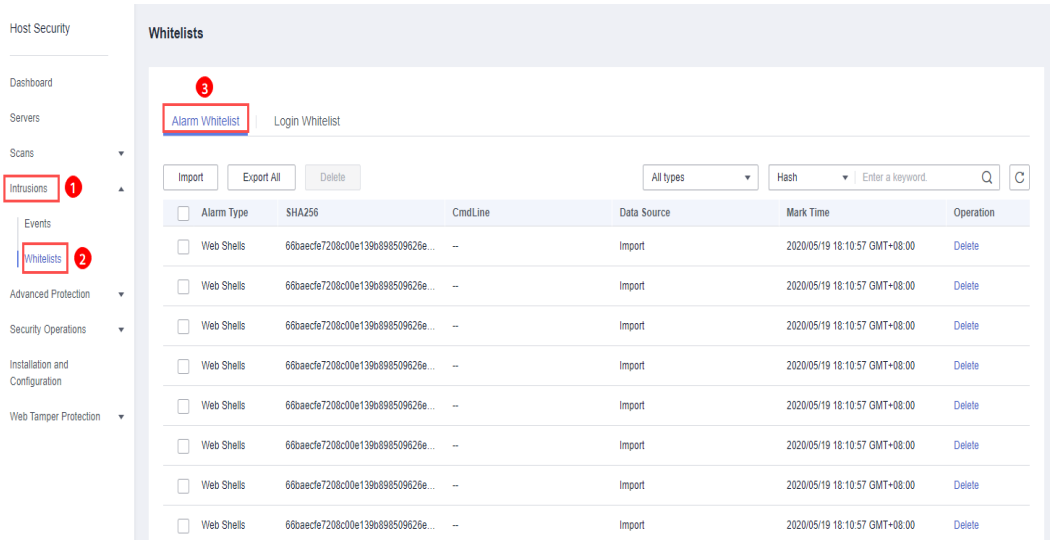
Perform the following steps to check the alarm whitelist:

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** > **Host Security Service**.

Step 3 On the **Whitelists** page, click **Alarm Whitelist**.

Figure 8-9 Alarm whitelist



----End

Importing and Exporting the Alarm Whitelist

You can import or export a whitelist for backup, restoration, or batch setting purposes.

NOTICE

- The exported alarm whitelist is in .csv format.
- The settings will fail to be imported if you opened the .csv file in Excel or changed the content format.

  Format:

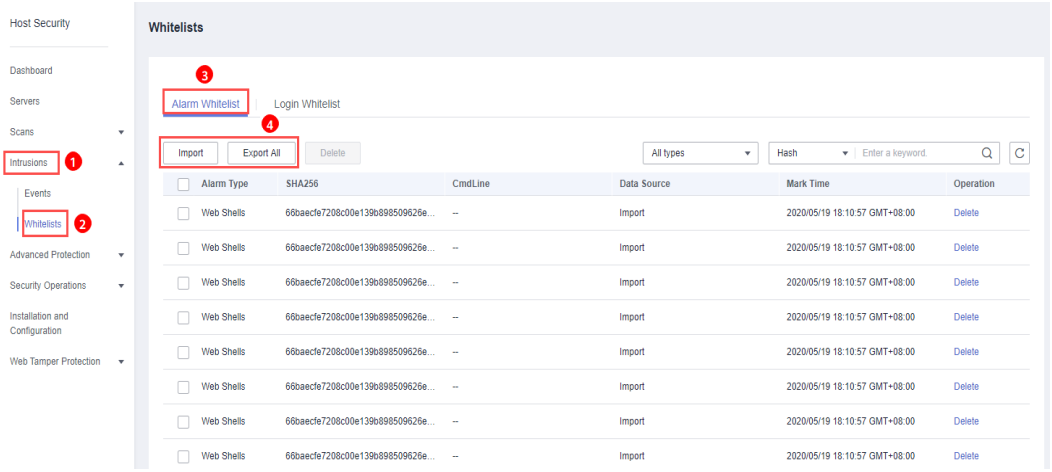
  "*Alarm_type*","*SHA256*","*Command_line*","*Data_source*","*Marking_time*"
  "webshell","66baecfe7208c00e139b898509626ee4d2ea81382ef15a4283b95d50f669b121","--","*File imported*","2020/02/28 07:32:44 GMT+08:00"
- The alarm whitelist supports incremental import. If the same record is imported again, only one entry will be displayed for it.

Step 1 Log in to the management console.

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

Step 3 On the **Whitelists** page, click the **Alarm Whitelist** tab, as shown in **Figure 8-10**.

Figure 8-10 Clicking the Alarm Whitelist tab



- Click **Export All** to export the current alarm whitelist as a .csv file.
- Click **Import** and select the exported Excel file to import the alarm whitelist.

  In the displayed dialog box, click **Upload** and select a file. After the import is complete, you can check the imported alarms in the whitelist.

  NOTE

  - Only the files in CSV, TXT, or UTF-8 format can be imported and exported.
  - The file size cannot exceed 5 MB.
  - The file name can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

----End

Follow-Up Procedure

Removing alarms from the whitelist

To remove an alarm from the whitelist, select it and click **Delete**.

NOTE

Alarms removed from the whitelist will be triggered. Removals cannot be rolled back. Exercise caution when performing this operation.

8.5 Configuring the Login Whitelist

To reduce false brute-force attack alarms, add trusted login IP addresses and their destination server IP addresses to the login whitelist.

On the **Login Whitelist** tab, you can add login IP addresses and usernames to the login whitelist of a specific server IP address. Whitelisted logins will not trigger alarms.

To add login information to the login whitelist, you can:

- Add false alarmed items of the **Brute-force attack** and **Abnormal login types** to the login whitelist when handling them. For details, see **Checking and Handling Intrusion Events**.
- Add it to the login whitelist on the **Login Whitelist** tab.

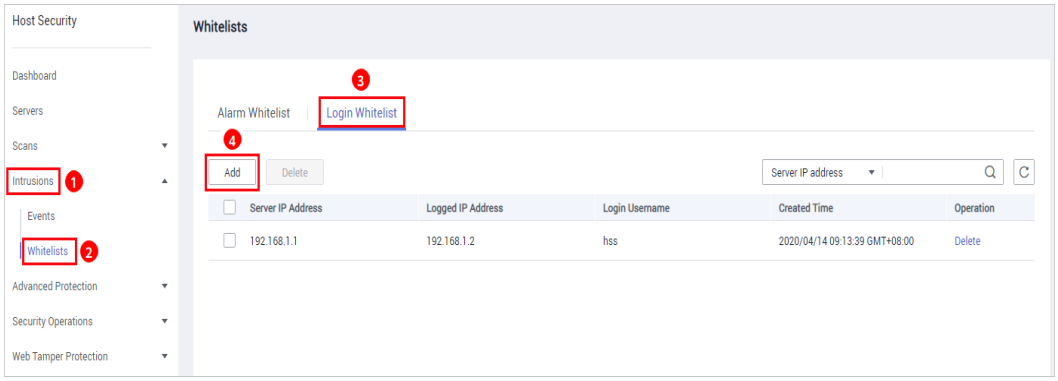
Adding Login Information to the Login Whitelist

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** > **Host Security Service**.

Step 3 On the **Whitelists** page, click the **Login Whitelist** tab and click **Add**, as shown in **Figure 8-11**.

Figure 8-11 Login whitelist

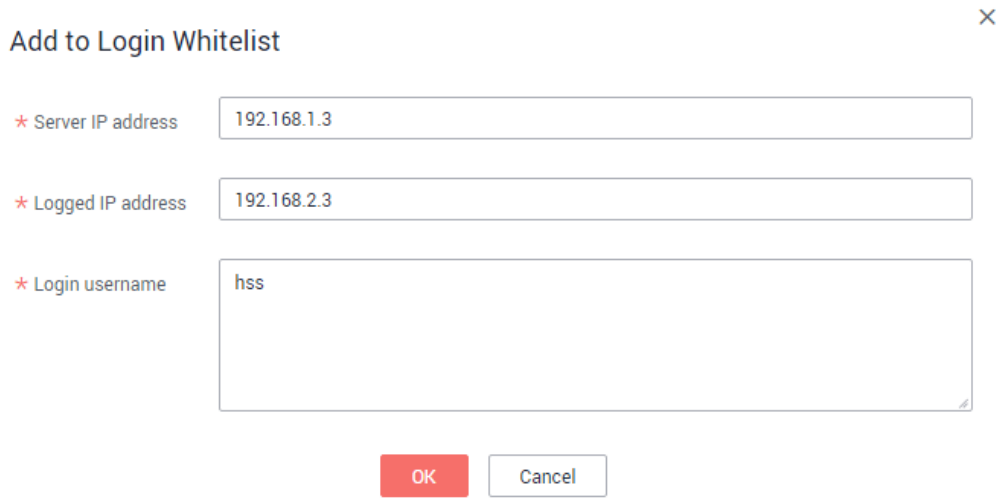


Step 4 In the **Add to Login Whitelist** dialog box, enter the server IP address, login IP address, and login username, as shown in **Figure 8-12**.

NOTE

- The IP addresses can be IPv4 or IPv6 addresses.
- You can enter one or more values in each IP address text box. IP addresses, ranges, and masks are supported, and should be separated by commas (,). Example: **192.168.1.1, 192.168.2.1-192.168.6.1, 192.168.7.0/24**.

Figure 8-12 Adding login information to the login whitelist



Step 5 Click **OK**.

----End

Other Operations

Removing login information from login whitelist

To delete a piece of login information from the whitelist, select it and click **Delete**, or click **Delete** in the row it resides.

NOTE

Exercise caution when performing the deletion operation because it cannot be rolled back.

9 Advanced Protection

9.1 Application Recognition Service

9.1.1 Checking the Whitelist Policy List

Application Recognition Service (ARS) scans all the applications running on your servers for uncertified or unauthorized applications, helping you maintain a secure runtime.

Function Description

Set whitelist policies, and determine whether applications are **Trusted**, **Untrusted**, or **Unknown**. The applications that are not whitelisted are not allowed to run. This function protects your servers from untrusted or malicious applications, reducing unnecessary resource usage.

You can create a whitelist policy and apply it to your servers. HSS will check whether suspicious or malicious processes exist on the servers, and generate alarms or isolate the processes that are not in the whitelist.

NOTE

- An alarm is generated when an application not in the whitelist is started.
- An application not in the whitelist is probably a new normal application, or a malicious program implanted through intrusion.
  - If the alarmed application is normal, frequently used, or a third-party application you installed, you are advised to add it to the whitelist. HSS will no longer report alarms when the application starts.
  - If the application is malicious, you are advised to delete it in a timely manner and check whether your configuration files, such as scheduled task files, have been tampered with.

Checking the Whitelist Policy 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** > **Host Security Service**.

Step 3 On the **Programs** page, click the **Whitelist Policies** tab, as shown in **Figure 9-1**.

Figure 9-1 Checking the whitelist policy list

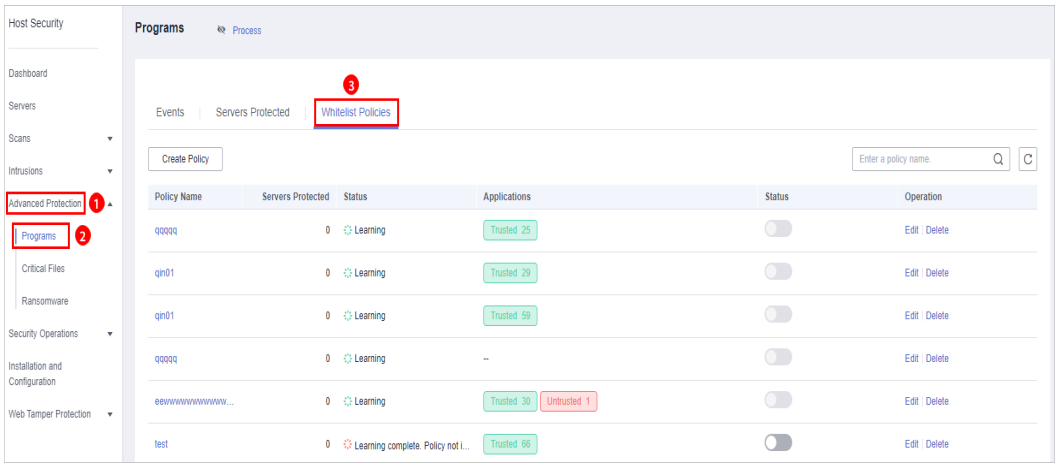


Table 9-1 Policy list parameters

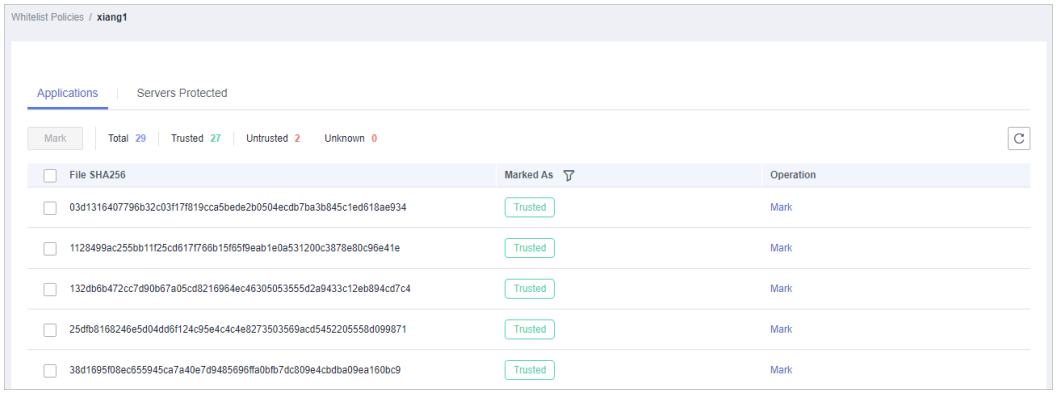
Parameter	Description
Policy Name	Whitelist policy name
Servers Protected	Number of servers where the whitelist policy takes effect
Status	Policy status. Its value can be: • Learning Intelligent learning is in progress. After a policy is created, the intelligent learning function automatically analyzes operations on the servers you selected. The status of a new policy is **Learning**. • Learning complete. Policy not in effect Intelligent learning is complete. You need to manually enable the policy for it to take effect. To enable the policy, click  in the row where it locates. HSS will automatically check whether the application running on your servers are trustworthy, and mark them as trusted, untrusted, or unknown. • Learning complete. Policy in effect Intelligent learning is complete. The policy has taken effect on associated servers.
Applications	Number of trusted, untrusted, and unknown applications identified by HSS

Parameter	Description
Switch	Enables or disables a policy. If the policy is in the **Learning complete. Policy not in effect** state, you can click  to enable it. The whitelist policy takes effect only after it is enabled.
Operation	Operations that can be performed on the policy, including: • **Applications**. You can click this button to select servers that a policy applies to. • **Edit**. You can click this button to modify the period and servers for intelligent learning. • **Delete**: You can click this button to delete a whitelist policy. After a whitelist policy is deleted, the applications on the servers associated to it will no longer be protected.

Step 4 Click the name of a whitelist policy to view the applications on associated servers, as shown in **Figure 9-2**.

The total number of applications, number of trusted applications, number of untrusted applications, and number of unknown applications are displayed. You can mark an application as trusted, untrusted, or unknown, and create an application whitelist for the application.

Figure 9-2 Application list

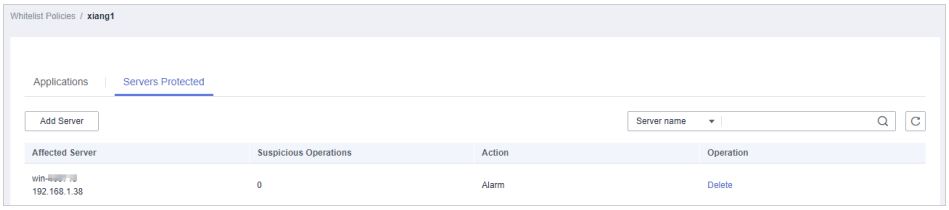


Step 5 Click the **Servers Protected** tab to view the servers that the whitelist policy applies to, as shown in **Figure 9-3**.

The server names and IP addresses, whitelist policy, number of suspicious operations, and the way to handle the operations are displayed.

- **Suspicious Operations** include startup of processes that are not in the whitelist policy or marked as **Untrusted** or **Unknown**.
- **Action** in the following figure indicates that HSS will report an alarm when detecting suspicious operations.

Figure 9-3 Checking protected servers



NOTE

You can remove servers as required. Servers removed will no longer be protected by the whitelist policy.

----End

9.1.2 Applying a Whitelist Policy

You can apply whitelist policies to your servers. A machine learning engine will automatically analyze operations performed on the servers. In this way, HSS will check whether suspicious or malicious processes exist on your servers, and report alarms on or isolate the processes that are not in the whitelist.

Prerequisites

- The premium edition has been enabled.
- The server you want to apply the policy to is in the **Running** state, its agent is in the **Online** state, and the premium edition has been enabled for the server.
- Only one whitelist policy can be applied to a server.

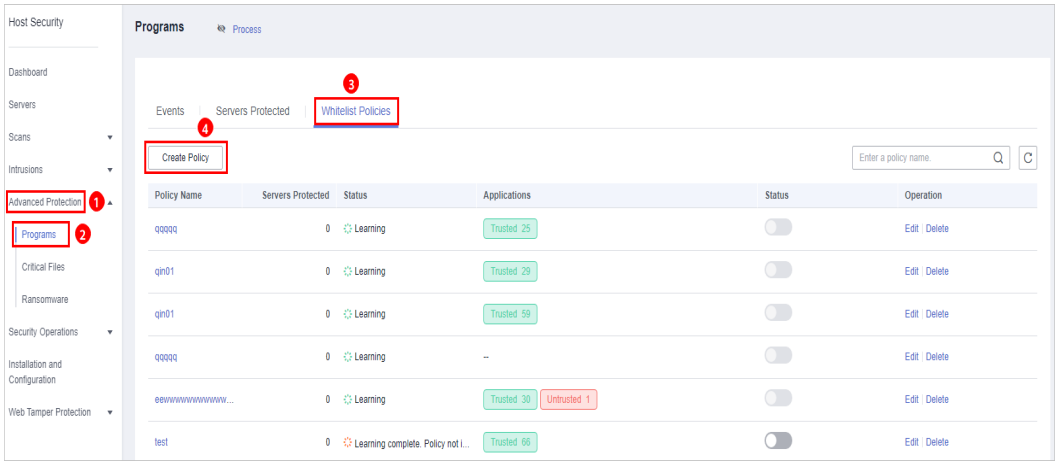
Creating a Whitelist Policy

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** > **Host Security Service**.

Step 3 On the **Programs** page, click the **Whitelist Policies** tab, and click **Create Policy**, as shown in **Figure 9-4**.

Figure 9-4 Creating a whitelist policy

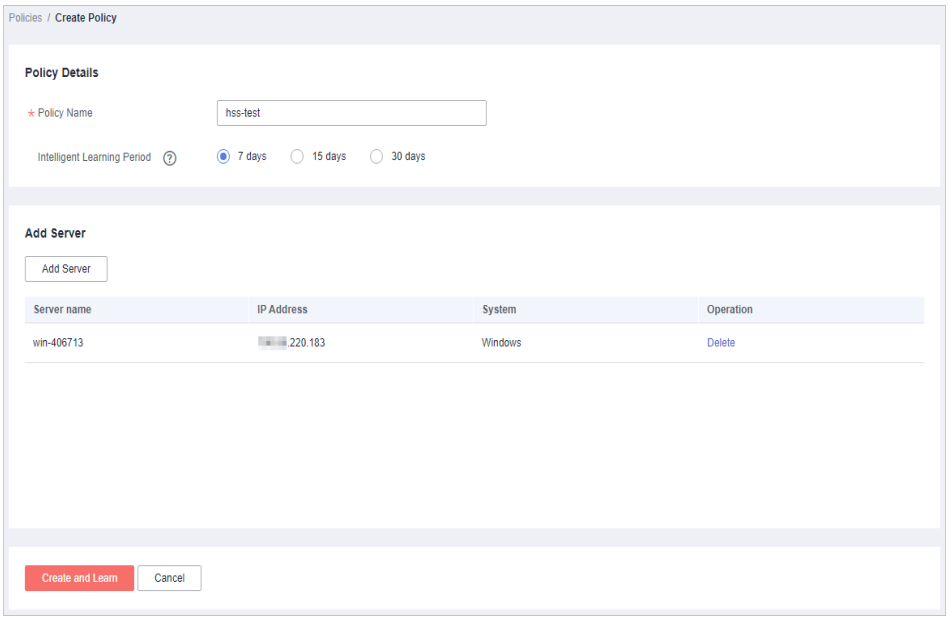


Step 4 Set policy details, as shown in **Figure 9-5**.

- **Policy Name**: Set a policy name.
- **Intelligent Learning Period**: Select **7 days**, **15 days**, or **30 days**.

  The period you select must be long enough for the policy to learn about all the common operations performed on your servers. Otherwise, intelligent learning results will be inaccurate.

Figure 9-5 Configuring a policy

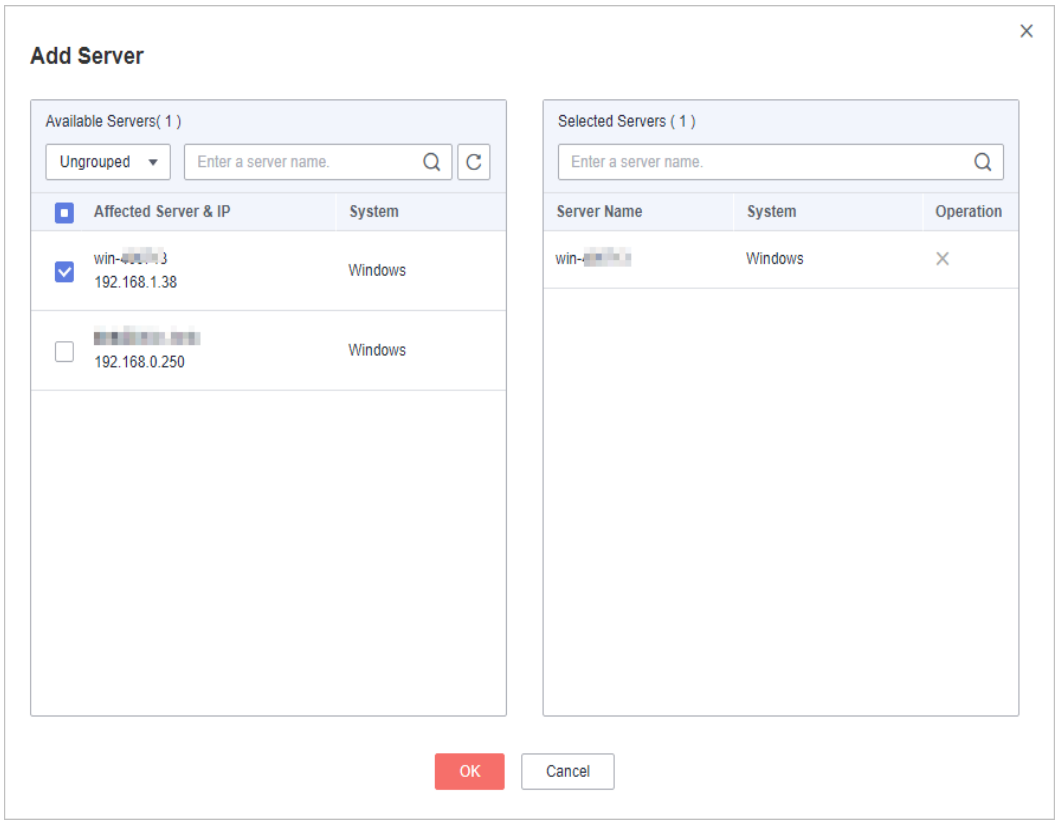


Step 5 Click **Add Server** to add an intelligent learning server, as shown in **Figure 9-6**.

NOTICE

- The server you want to apply the policy to must be in the **Running** state, its agent must be in the **Online** state, and the premium edition must be enabled for the server.
- You can add one or more servers. HSS will learn operations performed on them and identify trusted, untrusted, and unknown applications.

Figure 9-6 Adding servers for policy learning



Step 6 Click **OK**.

- In the server list, you can view the service name, IP address, and system of each server.
- You can add or remove learning servers as required.

Step 7 Click **Create and Learn**.

In the whitelist policy list, you can view the policy name, protected servers, policy status, applications, and whether a policy is enabled.

Step 8 Wait until the whitelist policy learning is complete and the policy status becomes **Learning complete. Policy not in effect**, and click to enable the whitelist policy.

After the whitelist policy is enabled, if its status becomes **Learning complete. Policy in effect**, the whitelist policy is successfully created.

----End

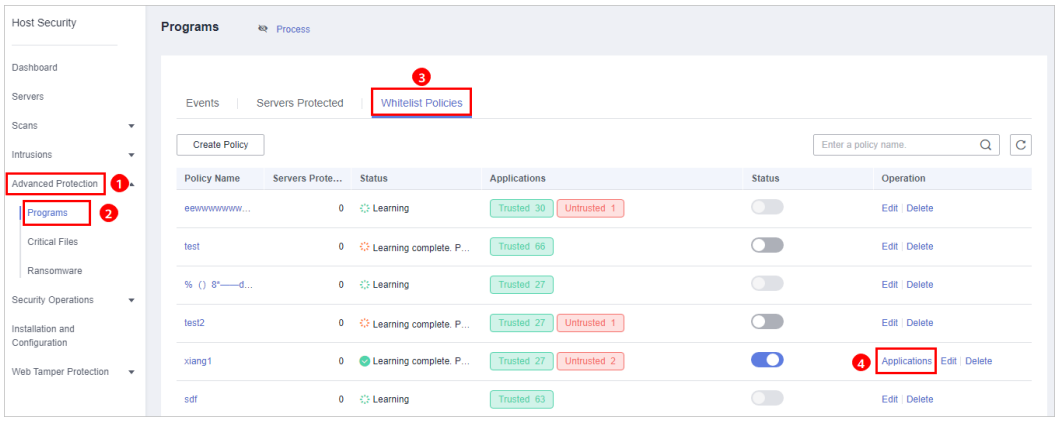
Associating Servers

After a whitelist policy is created, you can associate servers with it. HSS will check for suspicious or malicious processes on the associated servers.

You can only associate servers with a whitelist policy whose status is **Learning complete. Policy in effect**.

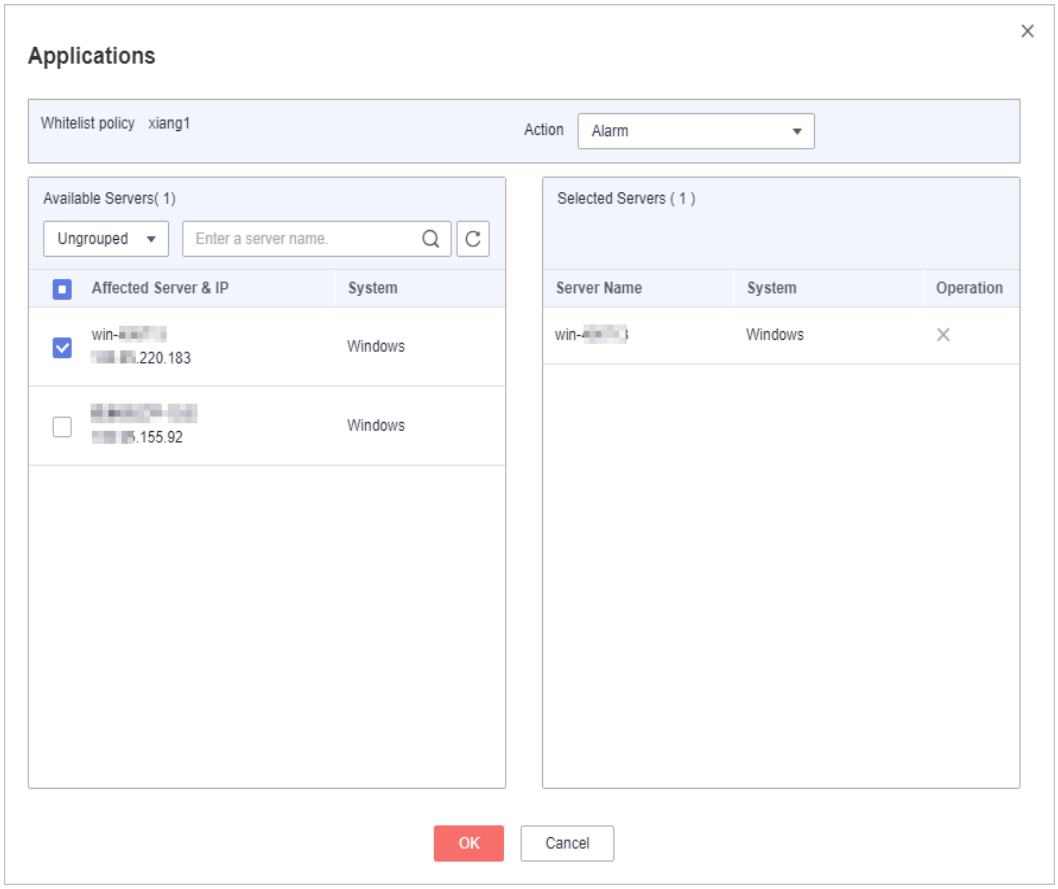
Step 1 Click **Applications**, as shown in **Figure 9-7**.

Figure 9-7 Associating servers



Step 2 In the displayed dialog box, select **Alarm** for **Action** and select servers, as shown in **Figure 9-8**.

Figure 9-8 Associating servers



Step 3 Click **OK**.

The number of servers associated with the whitelist policy will be displayed in the whitelist policy list.

----End

Follow-Up Procedure

Managing protected servers

- To add servers, click the **Servers Protected** tab and click **Add Server**.

  You can check the server names and IP addresses, whitelist policy, number of suspicious operations, and the way to handle the operations.
- To remove a protected server, click **Remove** in the **Operation** column. After a whitelist policy is deleted, the applications on the servers associated to it will no longer be protected.

Editing a whitelist policy

You can click **Edit** to modify the period and servers for intelligent learning.

Exercise caution when modifying the intelligent learning period of a policy. Before the learning completes, servers associated to the policy are not protected.

Deleting a whitelist policy

You can click the **Delete** button to delete a whitelist policy.

9.1.3 Checking and Handling Application Events

If a whitelist policy takes effect on your servers, HSS will check and mark applications as trusted, untrusted, or unknown, and report alarms on or isolate the applications that are not in the whitelist.

You can manually mark alarmed applications as trusted, untrusted, or unknown.

If you determine that a program is a malicious, you can manually isolate and kill it. When an application is isolated and killed, it is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious applications (if any).

The event management list displays untrusted and unknown applications, and the applications that are not in the whitelist policy.

NOTE

You are advised to check and handle the alarmed applications in a timely manner.

Checking Application 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** > **Host Security Service**.

Step 3 On the **Programs** page, click the **Events** tab, as shown in **Figure 9-9**.

Figure 9-9 Application event management page

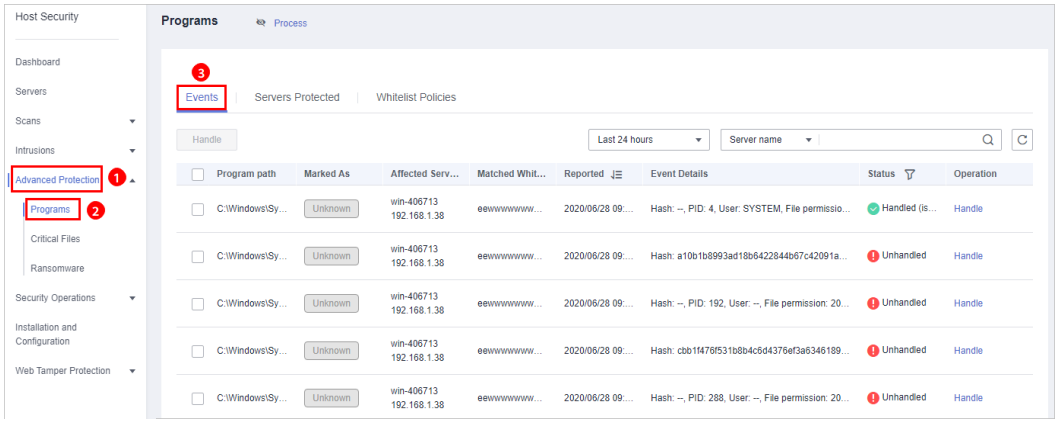


Table 9-2 Application event parameters

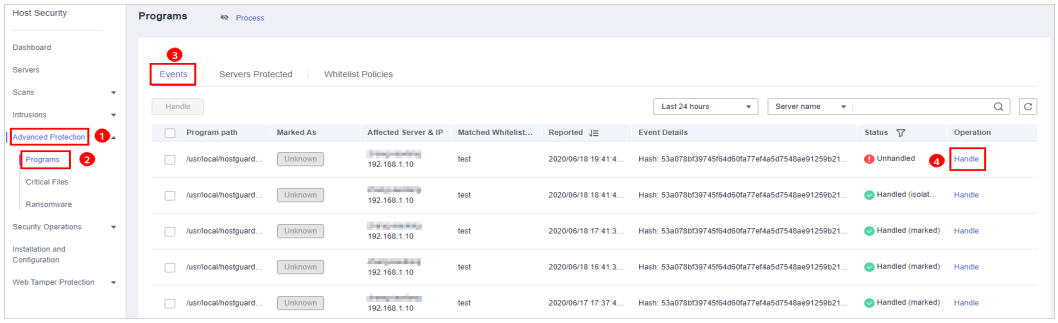
Parameter	Description
Program Path	Path of an application
Marked As	Application status. It can be **Trusted**, **Untrusted**, or **Unknown**.
Affected Server & IP	Name and IP address of an affected server
Matched Whitelist Policy	Whitelist policy that matches an alarm
Reported	Time when an alarm is reported
Event Details	Brief description of an alarm event
Status	Application event status. Its value can be **Handled** or **Unhandled**.

----End

Handling Application Events

Step 1 In the **Operation** column of an event, click **Handle**, as shown in **Figure 9-10**.

Figure 9-10 Handling an application event



Step 2 In the displayed **Handle Event** dialog box, select an action, as shown in **Figure 9-11**.

Figure 9-11 Handling an application event

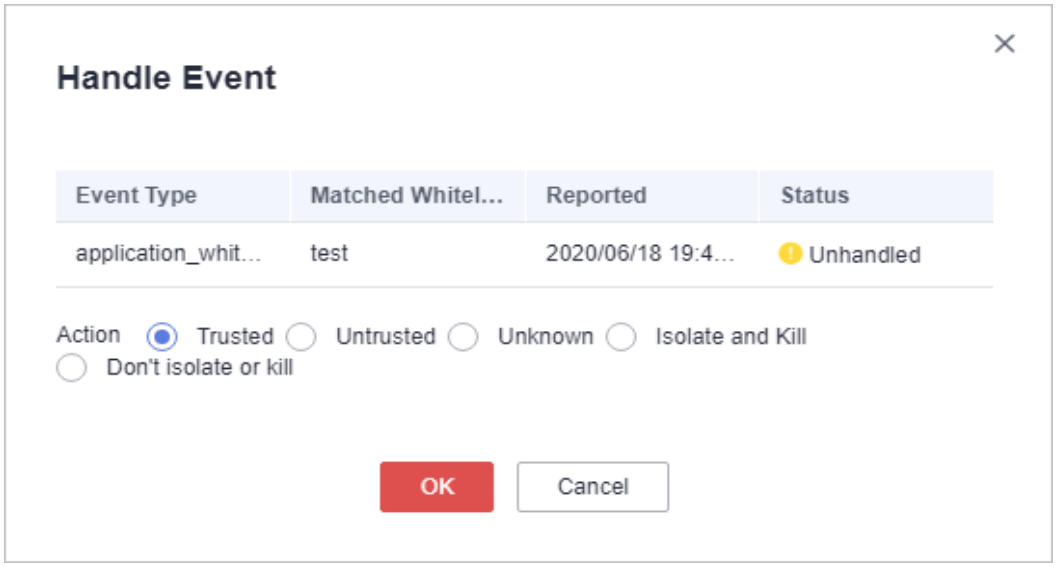


Table 9-3 Event handling actions

Action	Description
Trusted	Marks an application as trusted. The application startup will no longer trigger alarms.
Untrusted	Marks an application as untrusted. The application startup will trigger alarms.
Unknown	Marks an application as unknown. The application startup will trigger alarms.
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**. **NOTE** When an application is isolated and killed, it is terminated immediately. To avoid impact on services, check the detection result, and cancel the isolation of or unignore misreported malicious files (if any).
Don't isolate or kill	Cancels the isolation and killing of an application. **NOTE** Exercise caution when performing this operation. If you restore a malicious application, it will harm your servers.

Step 3 Click **OK**.

----End

9.2 File Integrity Monitoring

9.2.1 Adding a Monitored File

File integrity monitoring (FIM) checks the files in your OSs, applications, and other components for tampering, helping you meet PCI-DSS requirements.

FIM compares files with their versions in the previous scan to check whether files have been modified, and whether the modifications are suspicious.

FIM checks the integrity of Linux files and manages operations on them, including:

- Create and delete files
- Modify files (changes in file size, ACLs, and content hashes)

The registry monitoring function will be available soon.

NOTICE

You are advised to monitor only the files that are important for systems and applications, and are rarely modified.

If you monitor files that are frequently modified, by applications or OSs, such as log files and text files, a lot of false alarms will be generated.

Enabling FIM

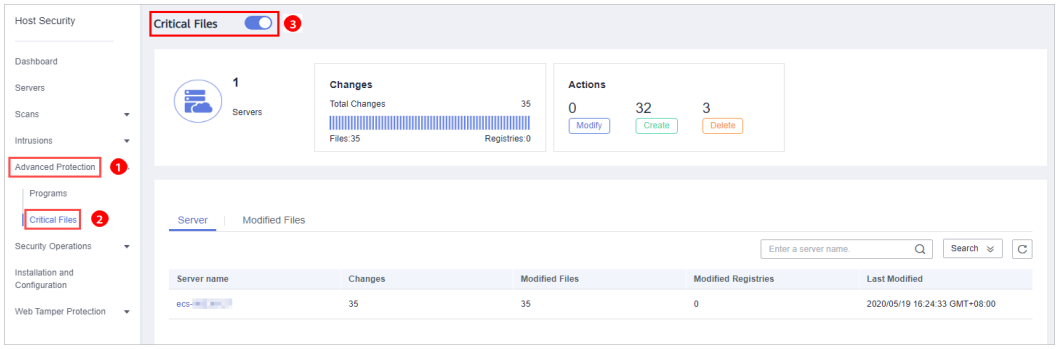
Step 1 Log in to the management console.

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

Step 3 On the **Critical Files** page, click  to enable FIM, as shown in **Figure 9-12**.

The default setting is  .

Figure 9-12 Enabling FIM



Step 4 Check the total number of servers, number of modified files, types of modifications, risks, affected servers, and modified files.

----End

Adding a Monitored File

To add a management file, ensure that:

- You have deployed the **Integrity check on critical files** policy on servers.
- The **Integrity check on critical files** policy has been enabled.

Perform the following steps to add a monitored file:

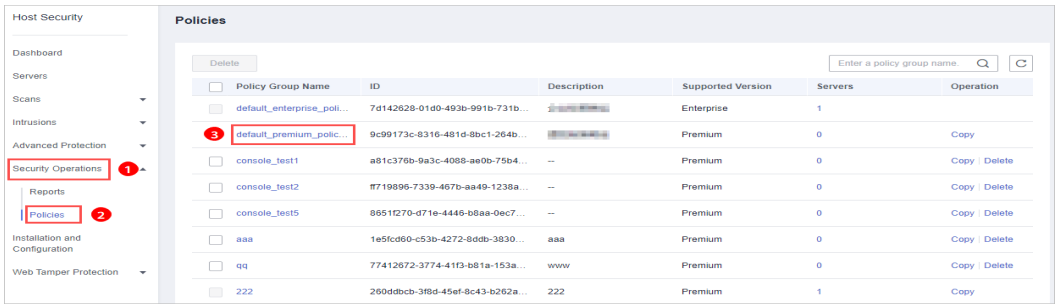
Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Security Operations** > **Policies**.

Step 4 On the **Policies** page, click the policy group deployed on your servers. Take the **default policy group of the premium edition** group as an example, as shown in **Figure 9-13**.

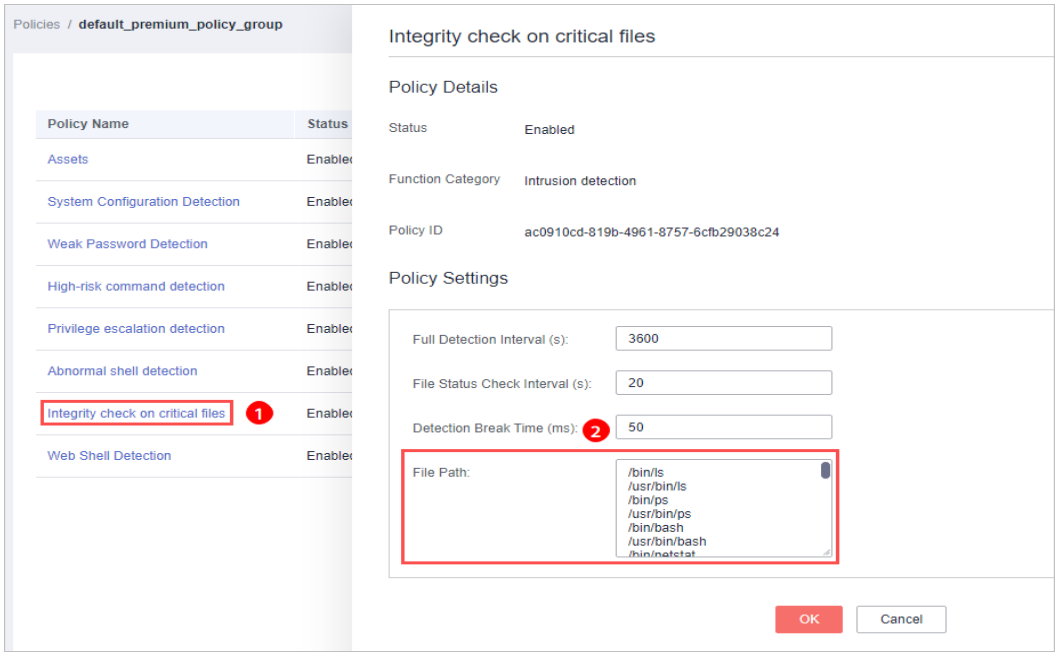
Figure 9-13 Default policy group



Step 5 Click **Integrity check on critical files** and set monitored files, as shown in **Figure 9-14**.

For details about how to configure the **Integrity check on critical files** policy, see **File Integrity Monitoring**.

Figure 9-14 Opening the **Integrity check on critical files** policy



Step 6 Click **OK**.

----End

Follow-Up Procedure

Disabling FIM

To disable FIM, click . If the function is disabled, HSS no longer monitors your files or displays FIM statistics.

9.2.2 Checking Change Statistics

You can check the number and types of changes, the number of modified files and registries on a server, and change details to find malicious changes in a timely manner.

Checking Change Statistics

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** > **Host Security Service**.

Step 3 Go to the **Critical Files** page to check change statistics, as shown in **Figure 9-15**.

Figure 9-15 Checking change statistics

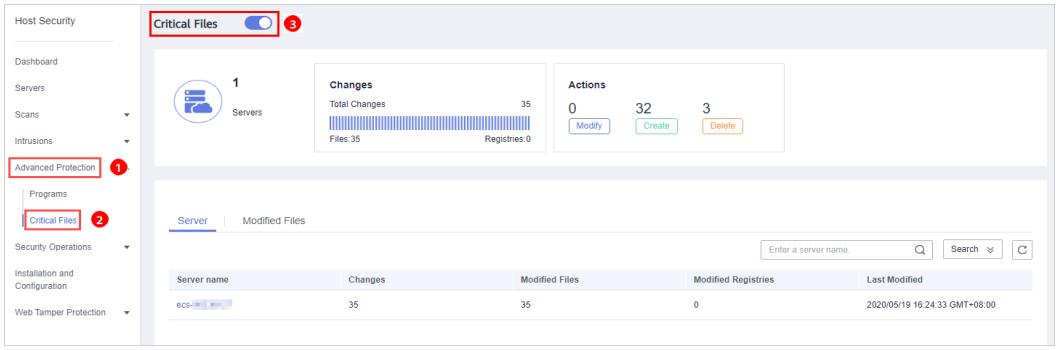


Table 9-4 Change statistics

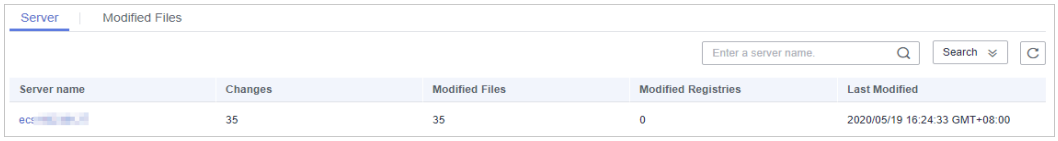
Item	Description
Servers	Total number of managed servers
Changes	• **Changes**: total number of modifications in monitored files • **Files**: total number of files • **Registries**: total number of registries
Actions	• **Modify**: total number of changes in monitored files • **Create**: total number of created files • **Delete**: total number of deleted files

----End

Checking Modified Files on a Single Server

Step 1 In the server list, check modified files and registries on a server, and the time when they were modified.

Figure 9-16 Server list

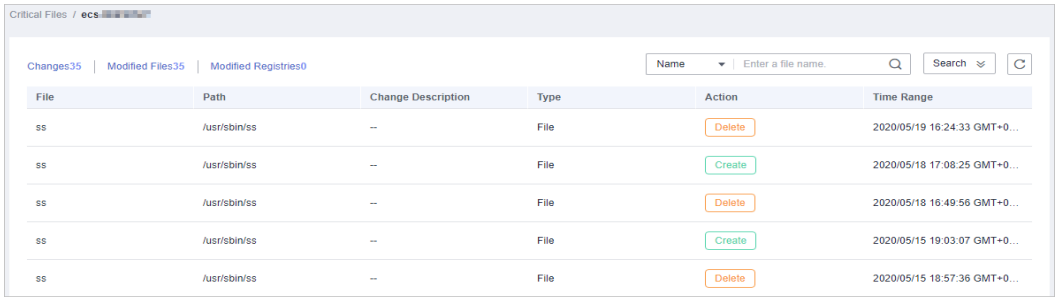


Step 2 Click a server name and check its change statistics above the displayed list, including the total number of changes, number of modified files, and number of modified registries, as shown in **Figure 9-17**.

NOTE

You can click **Search** to expand the advanced search area. Here you can search for a server by its name and the time when changes were made.

Figure 9-17 Server change details



Step 3 Check the change details of the files and registries in the file list of the server.

The details include including the file and registry names and types, paths, changed content, actions, and time when changes were made.

NOTE

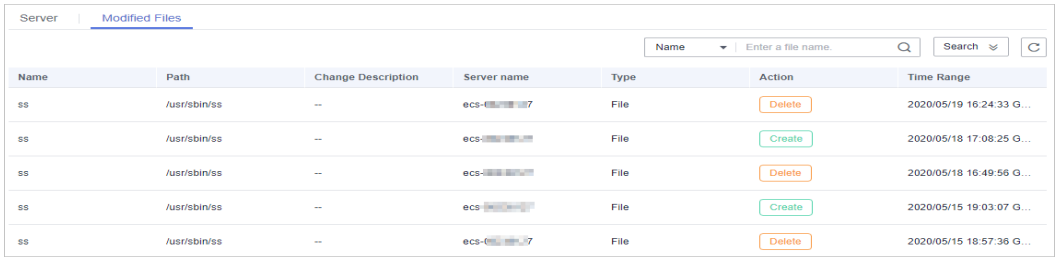
- You can enter a name or path to search for a file or registry.
- You can click **Search** to expand the advanced search area. Here you can search for a server by **Name**, **Path**, **Type**, **Action**, and **Time Range**.

----End

Checking All the Modified Files

You can check all the change files and registries on your servers, including their names, paths, description, server names, actions, and the time when they were changed, as shown in **Figure 9-18**.

Figure 9-18 Changed files



NOTE

- You can enter a name or path to search for a file or registry.
- You can click **Search** to expand the advanced search area. Here you can search for a server by **Name**, **Path**, **Type**, **Action**, and **Time Range**.

9.3 Ransomware Prevention

9.3.1 Checking Protection Policies

HSS monitors critical files stored on your servers and prevents unauthorized applications from encrypting or modifying the files, protecting your servers from ransomware.

You can create ransomware prevention policies and configure the protection status, monitored file path, and associated servers for the policy. A machine learning engine is used to identify whether an application has possibly tampered with any of the files on your servers. After the learning completes, the policy automatically takes effect on associated servers.

The policy analyzes operations on servers, identifies trusted applications, and reports alarms on untrusted applications.

Prerequisites

- The servers you want to protect run the Windows OS.
- The server is in the **Running** state, and its agent is in the **Online** state.

Checking the Policy 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** > **Host Security Service**.

Step 3 On the **Ransomware** page, click the **Policies** tab. The ransomware prevention policy list is displayed, as shown in **Figure 9-19**.

Figure 9-19 Policy list

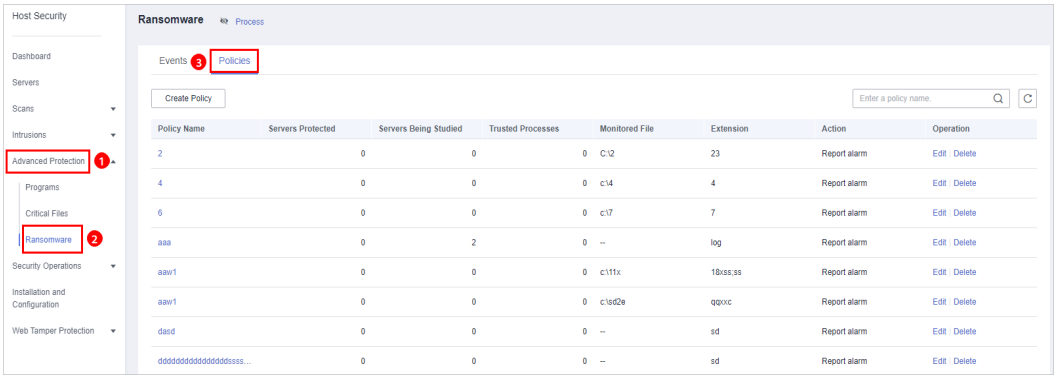


Table 9-5 Policy parameters

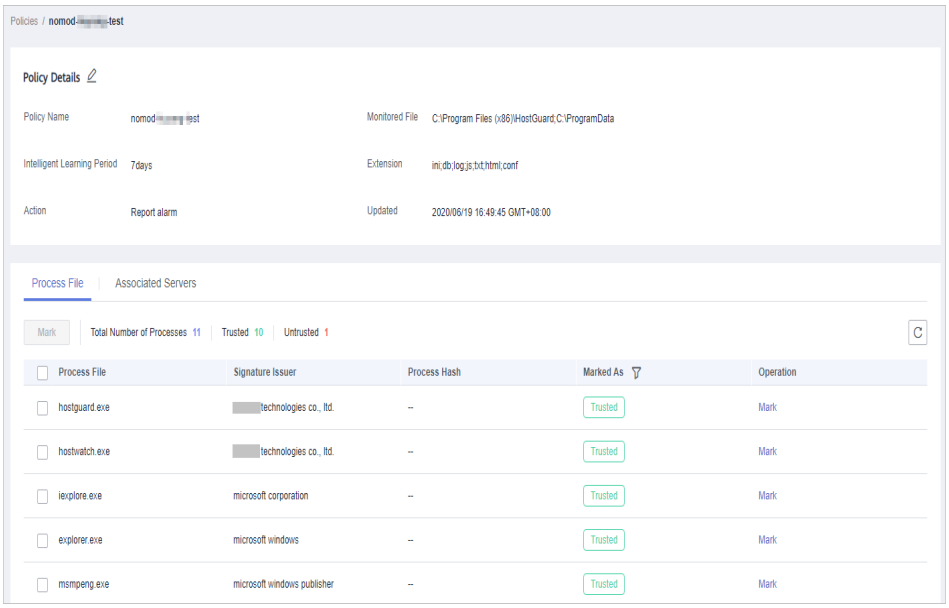
Parameter	Description
Policy Name	Policy name
Servers Protected	Number of servers where the policy takes effect
Servers Being Studied	Servers where intelligent learning is in progress. The status of a new policy is **Learning**.
Trusted Processes	Number of trusted processes automatically identified by HSS

Parameter	Description
Monitored File	Path of monitored files. Multiple paths are separated by semicolons (;). Operations on the files in these paths are monitored. If no paths are specified, all the files on the servers associated to the policy are monitored.
Extension	Extensions of monitored files
Action	Action taken when suspicious operations on monitored files are detected. For example, report alarms.

Step 4 Click a policy name to check its details and process files, as shown in **Figure 9-20**.

- You can check the policy name, intelligent learning period, protection status, monitored file path, file name extension, and update time.
- You can check the total number of processes, number of trusted processes, number of untrusted processes, process files, signature issuer, process hash, and trust status.
- You can mark a process file as **Trusted** or **Untrusted**. An alarm will be generated if an untrusted process is started.

Figure 9-20 Protection policy details



Step 5 Click **Associated Servers** to check servers associated to the policy, as shown in **Figure 9-21**.

Figure 9-21 Checking associated servers

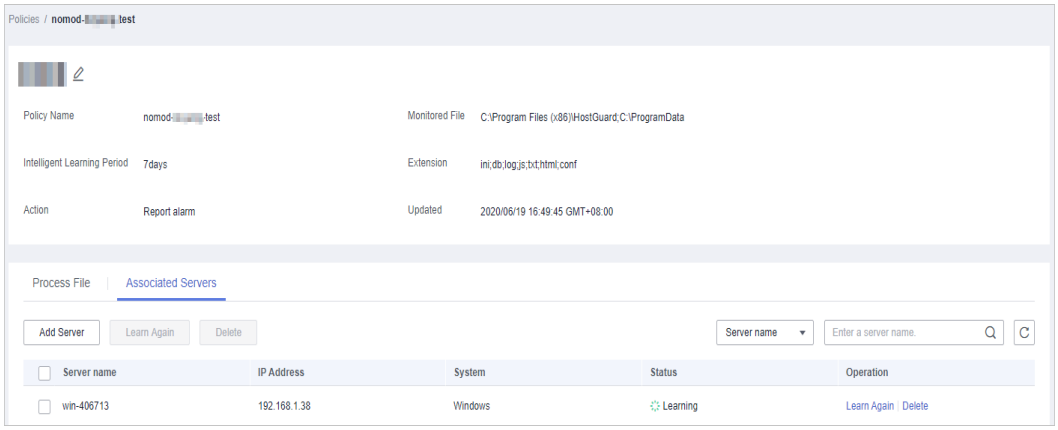


Table 9-6 Associated servers

Parameter	Description
Server Name	Server name
IP Address	Server IP address
System	Server OS. Only Windows OSs can be protected.
Status	Policy status. Its value can be: • Learning Intelligent learning is in progress. After a policy is created, the intelligent learning function automatically analyzes operations on associated servers. The status of a new policy is **Learning**. • Learning complete. Policy in effect Intelligent learning is complete. The policy has taken effect on associated servers.

Parameter	Description
Operation	Operations that can be performed on the policy, including: • Learn Again – If any software you use was greatly modified, learning must be performed again on associated servers. Click **Learn Again**. – If intelligent learning period you set is too short, learning results will be inaccurate. If the learning still continuous after the period expires, the policy status will remain **Learning**. In these cases, set **Intelligent Learning Period** to a proper duration and click **Learn Again**. – If the server is in **Stopped** or **Faulty** state, the agent is in **Offline** state, or the premium edition is disabled during learning, learning will be interrupted. The policy status will still be **Learning**, but the system will not respond if you click **Learn Again**. In this case, ensure the server is in **Running** state, the agent is in **Online** state, and the premium edition is enabled for the server, and click **Learn Again**. • Delete Removes an associated server. Files on the server will no longer be protected by the policy.

----End

9.3.2 Creating a Protection Policy

To protect your servers from ransomware, you can create a policy, set critical file paths in the policy, and enable machine learning.

Machine learning automatically collects and aggregates normal application behavior on the servers associated with the policy. Operations on files performed by untrusted applications or applications that are not specified in the policy will trigger alarms.

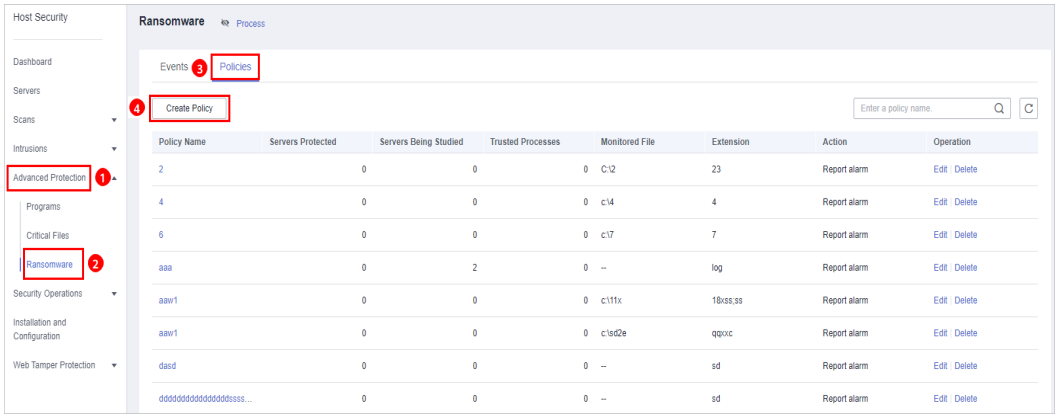
Creating a Protection Policy

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** > **Host Security Service**.

Step 3 On the **Ransomware** page, click the **Policies** tab, and click **Create Policy**, as shown in **Figure 9-22**.

Figure 9-22 Policy management



Step 4 Set policy details, as shown in **Figure 9-23**.

Figure 9-23 Configuring a ransomware prevention policy

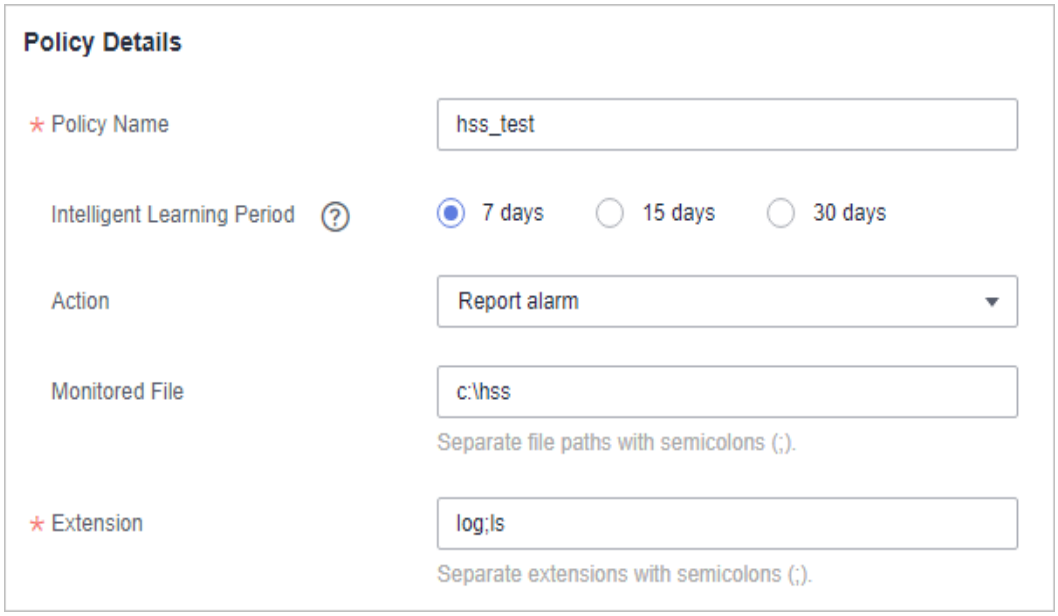


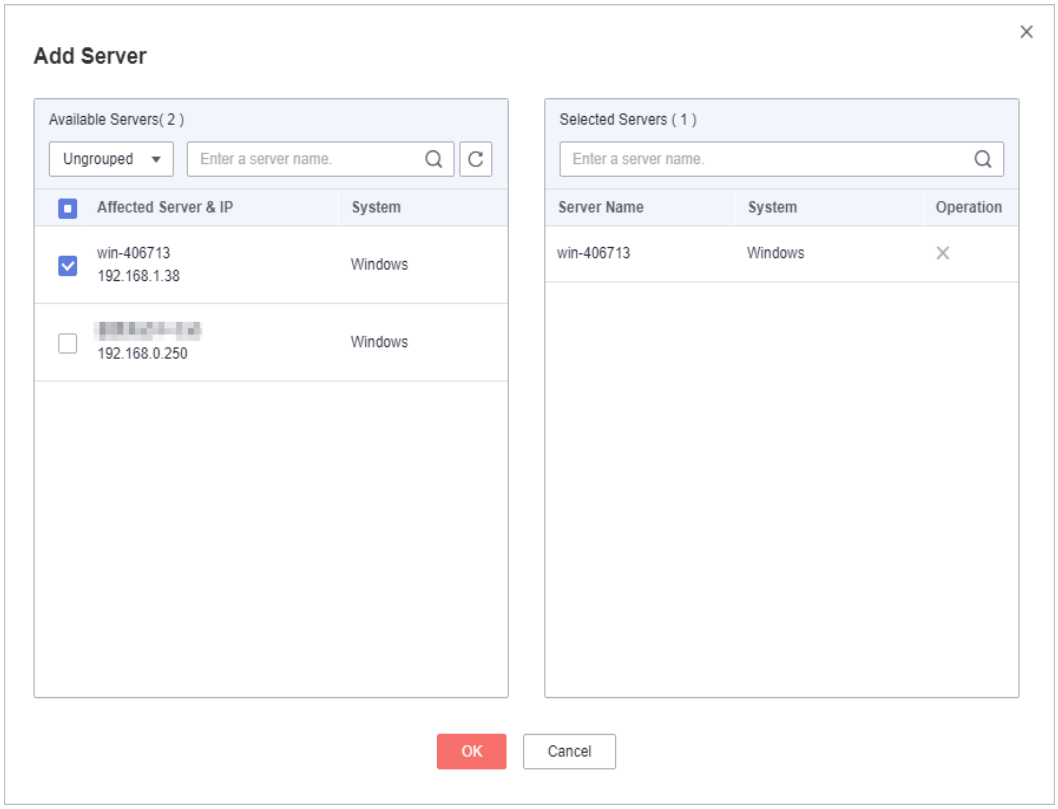
Table 9-7 Basic information parameters

Parameter	Description
Policy Name	Ransomware prevention policy name
Intelligent Learning Period	Select **7 days**, **15 days**, or **30 days**. HSS uses a machine learning engine to identify if an application has possibly tampered with any of the files on your servers.
Action	Action taken when suspicious operations on monitored files are detected. For example, report alarms.

Parameter	Description
Monitored File	Path of monitored files. Multiple paths are separated by semicolons (;). Operations on the files in these paths are monitored. If no paths are specified, all the files on the servers associated to the policy are monitored.
Extension	Extension of monitored files. Multiple paths are separated by semicolons (;).

Step 5 Click **Add Server**. In the displayed **Add Server** dialog box, select associated servers, as shown in **Figure 9-24**.

Figure 9-24 Associating servers



Step 6 Click **OK**.

NOTE

- You can check the name, IP address, and system of the associated server.
- To remove an associated server, click **Delete** in the **Operation** column.

Step 7 Click **Create and Learn**.

Created policies will be displayed in the policy list, as shown in **Figure 9-25**.

Figure 9-25 Ransomware prevention policy list

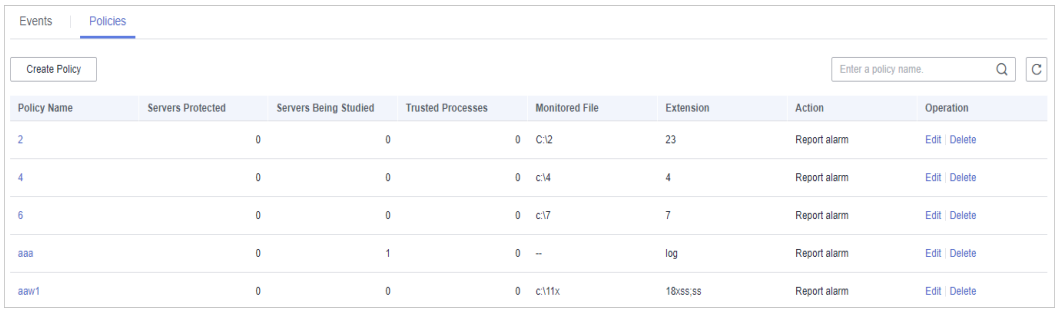


Table 9-8 Policy list parameters

Parameter	Description
Policy Name	Intelligent learning policy name
Servers Protected	Number of servers protected by the policy
Servers Being Studied	Number of servers where the learning is performed
Trusted Processes	Number of trusted processes. After the intelligent learning policy takes effect, HSS automatically identifies and counts trusted processes on your server.
Monitored File	Path of monitored files. Multiple paths are separated by semicolons (;). Operations on the files in these paths are monitored. If no paths are specified, all the files on the servers associated to the policy are monitored.
Extension	Extension of monitored files. Multiple paths are separated by semicolons (;).
Action	Action taken when suspicious operations on monitored files are detected. For example, report alarms.

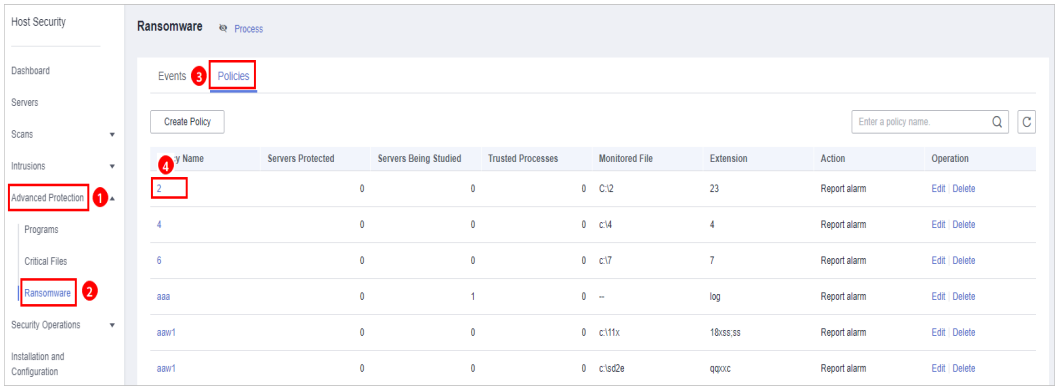
----End

Associating Servers

You can associated servers to an existing intelligent learning policy on the **Associated Servers** tab on the policy details page.

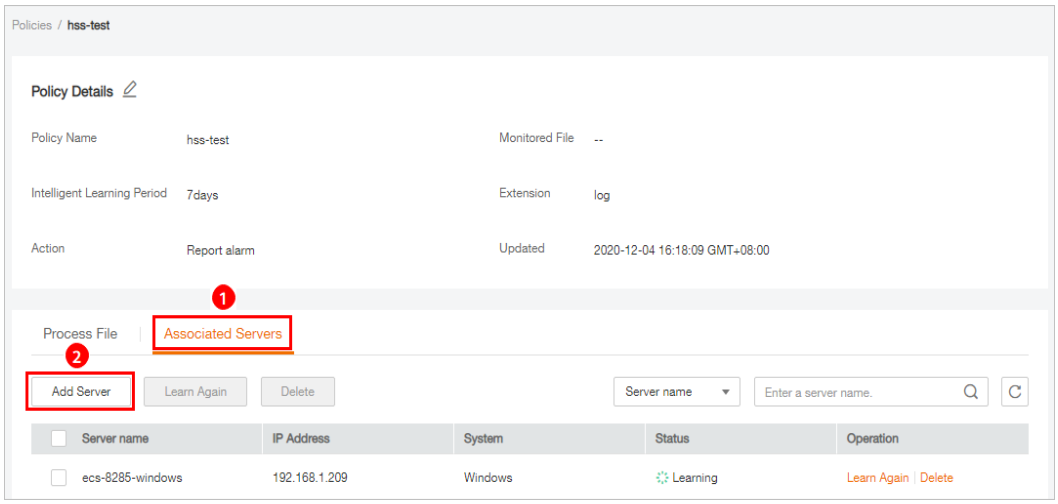
Step 1 Click the name of a policy. The policy details page is displayed, as shown in **Figure 9-26**.

Figure 9-26 Accessing the policy details page



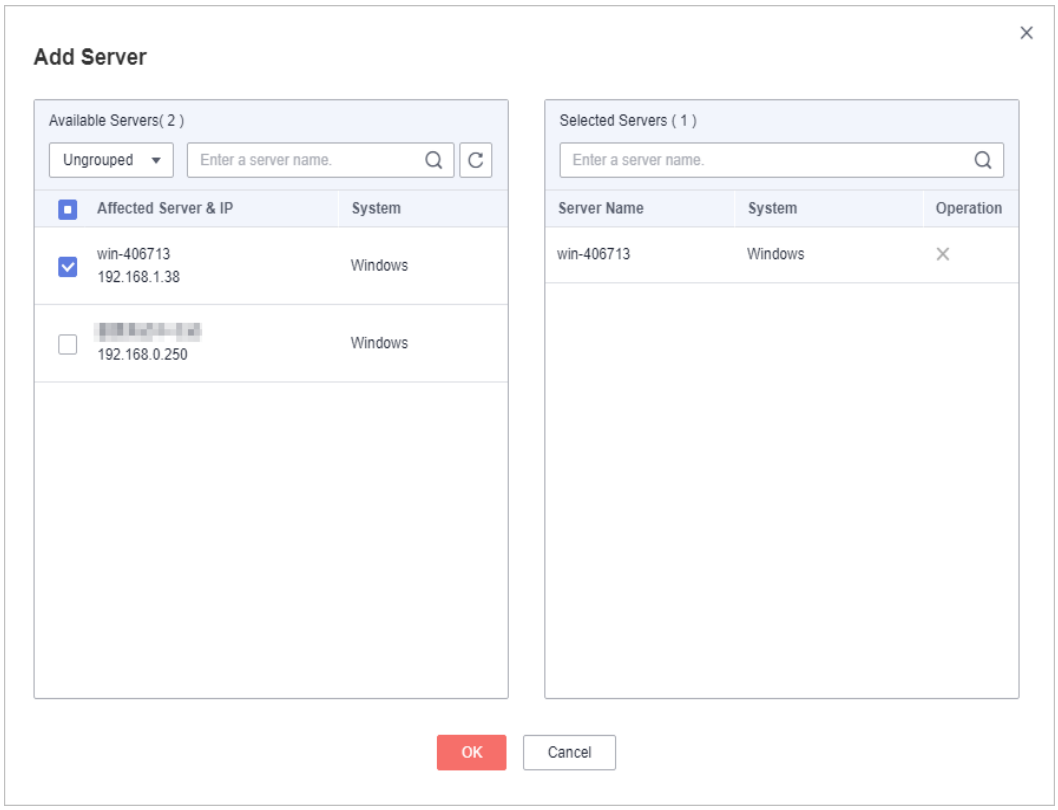
Step 2 Click the **Associated Servers** tab and click **Add Server**, as shown in **Figure 9-27**.

Figure 9-27 Adding associated servers



Step 3 In the displayed **Add Server** dialog box, select servers, as shown in **Figure 9-28**.

Figure 9-28 Associating servers



Step 4 Click **OK**.

After associated servers are added, you can check their server names, IP addresses, systems, and policy. By default, the initial policy status is **Learning**.

After the learning is complete, the policy status changes to **Learning complete. Policy in effect**. The ransomware prevention policy will automatically take effect on all servers associated with it.

----End

Follow-Up Procedure

Editing a policy

You can click **Edit** to modify the policy name, intelligent learning period, protection status, monitored file paths, and file extensions.

Deleting a policy

You can click the **Delete** button to delete a policy. Servers associated with it will no longer be protected.

9.3.3 Checking and Handling Protection Events

If a ransomware protection policy takes effect on servers, HSS will check operations performed on monitored files on the servers, mark the operations as trusted or untrusted, and report alarms on operations performed by the applications that are untrusted or not specified in the policy.

The event management page displays untrusted operations that match a policy and operations performed by that applications that are not specified in any policies.

NOTE

You are advised to pay attention to these events and handle them in a timely manner.

Checking 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** > **Host Security Service**.

Step 3 On the **Ransomware** page, click the **Events** tab, as shown in **Figure 9-29**.

Figure 9-29 Ransomware prevention events

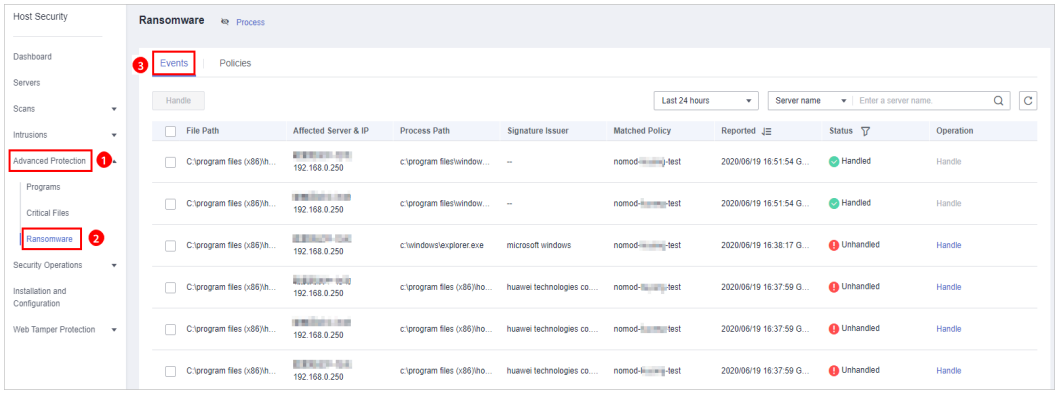


Table 9-9 Ransomware prevention event parameters

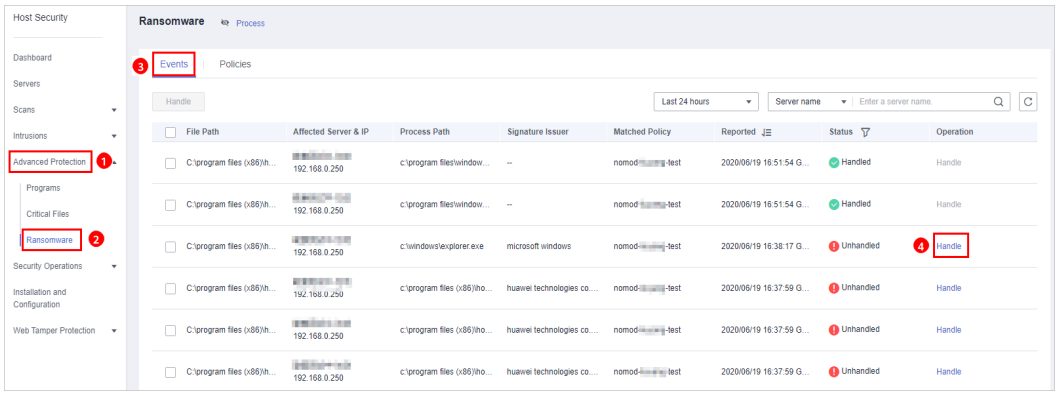
Parameter	Description
File Path	Path of the file operated by an application
Affected Server & IP	Name and IP address of the server where the file operation is performed
Process Path	Path of the Application that performs operations on files
Signature Issuer	Signature issuer
Matched Policy	Policy that matches the alarm
Reported	Time when an alarm is reported
Status	Event status. Its value can be **Handled** or **Unhandled**.

----End

Handling Ransomware Prevention Events

Step 1 In the **Operation** column of an event, click **Handle**, as shown in **Figure 9-30**.

Figure 9-30 Checking ransomware prevention events



Step 2 In the displayed dialog box, select **Trusted** or **Untrusted**, as shown in **Figure 9-31**.

Figure 9-31 Handling ransomware events

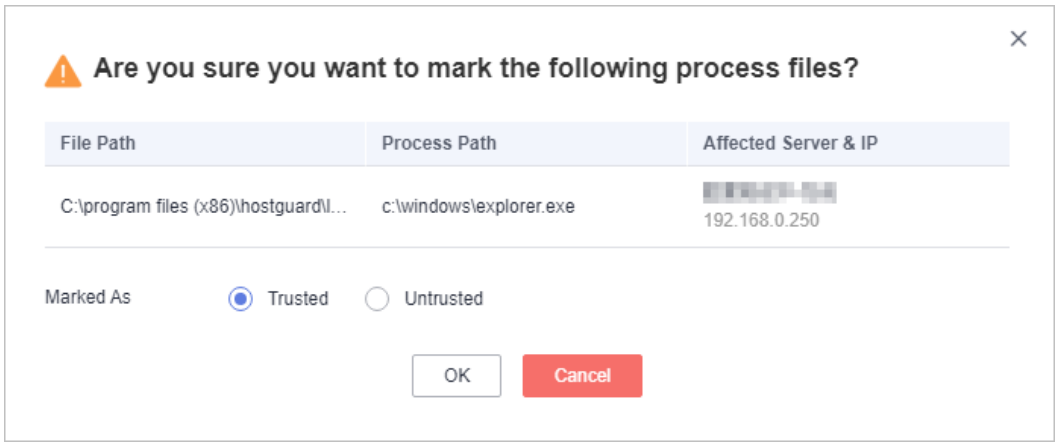


Table 9-10 Event handling parameters

Marked As	Description
Trusted	An application marked as trusted will not trigger alarms if it performs operation on files under monitored paths.
Untrusted	An application marked as untrusted will trigger alarms if it performs operation on files under monitored paths.

Step 3 Click **OK**.

----End

10 Security Operations

10.1 Checking or Creating a Policy Group

You can group policies and servers to batch apply policies to servers, easily adapting to business scenarios.

Precautions

- When you enable the enterprise edition, the default policy group of this edition (including weak password and website shell detection policies) takes effect for all your servers.
- When you enable the premium or WTP edition, the edition is bound to **default_premium_policy_group**.

  To create your own policy group, you can copy the default policy group and add or remove policies in the copy.

Policy List

Policy	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition
Weak password detection	Change weak passwords to stronger ones based on HSS scan results and suggestions.	Linux and Windows	√ (Check only custom weak passwords)	√	√

Policy	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition
Web shell detection	Scan web directories on servers for web shells.	Linux and Windows	√ (Check only specified detection paths)	√	√
Assets	Scan and display all software in one place, including software name, path, and major applications, helping you identify abnormal assets.	Linux and Windows	×	√	√
System configuration detection	Check for unsafe Tomcat, Nginx, and SSH login configurations.	Linux and Windows	×	√	√
High-risk command detection	Check executed commands in real time and generate alarms if high-risk commands are detected.	Linux	×	√	√

Policy	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition
Privilege escalation detection	Detect privilege escalation for processes and files in the current system. The following abnormal privilege escalation operations can be detected: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities • File privilege escalation	Linux	×	√	√
Abnormal shell detection	Detect actions on abnormal or reverse shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.	Linux	×	√	√
File integrity monitoring	Check the files in the Linux OS, applications, and other components to detect tampering.	Linux	×	√	√

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** > **Host Security Service**.

Step 3 In the navigation pane, choose **Security Operations** > **Policies**.

----End

Checking the Policy Group List

Step 1 Go to the **Policies** page, as shown in **Figure 10-1**. For more information, see **Table 10-1**.

NOTE

- **default_enterprise_policy_group** is the default policy group of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted.
- **default_premium_policy_group** is the default policy group of the premium edition. You can create a policy group by copying this default group and modify the copy.
- To refresh the list, click in the upper right corner.
- To view details about the servers associated with a policy group, click the number in the **Servers** column of the group.

Figure 10-1 Policy group list

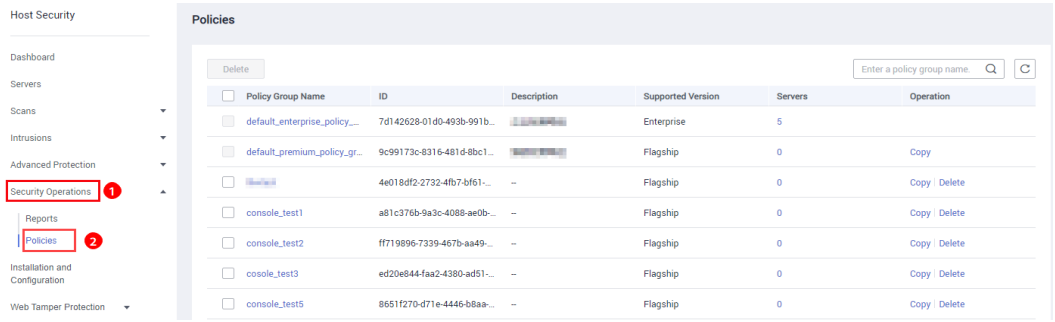


Table 10-1 Policy group parameters

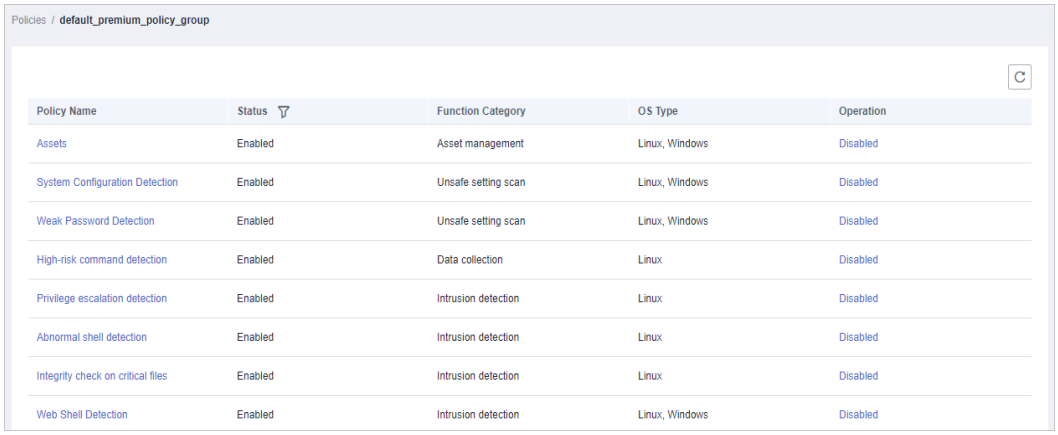
Parameter	Description
Policy Group Name	Name of a policy group
ID	Unique ID of a policy group
Description	Description of a policy group
Supported Version	HSS edition supported by a policy group

Step 2 Click the name of a policy group to check policy details, including the names, statuses, function categories, OS type of the policies, as shown in **Figure 10-2**.

NOTE

- By default, all policies in the groups **default_enterprise_policy_group** and **default_premium_policy_group** are enabled.
- You can click **Enable** or **Disable** in the **Operation** column of a policy to control what to check.

Figure 10-2 Policy group details

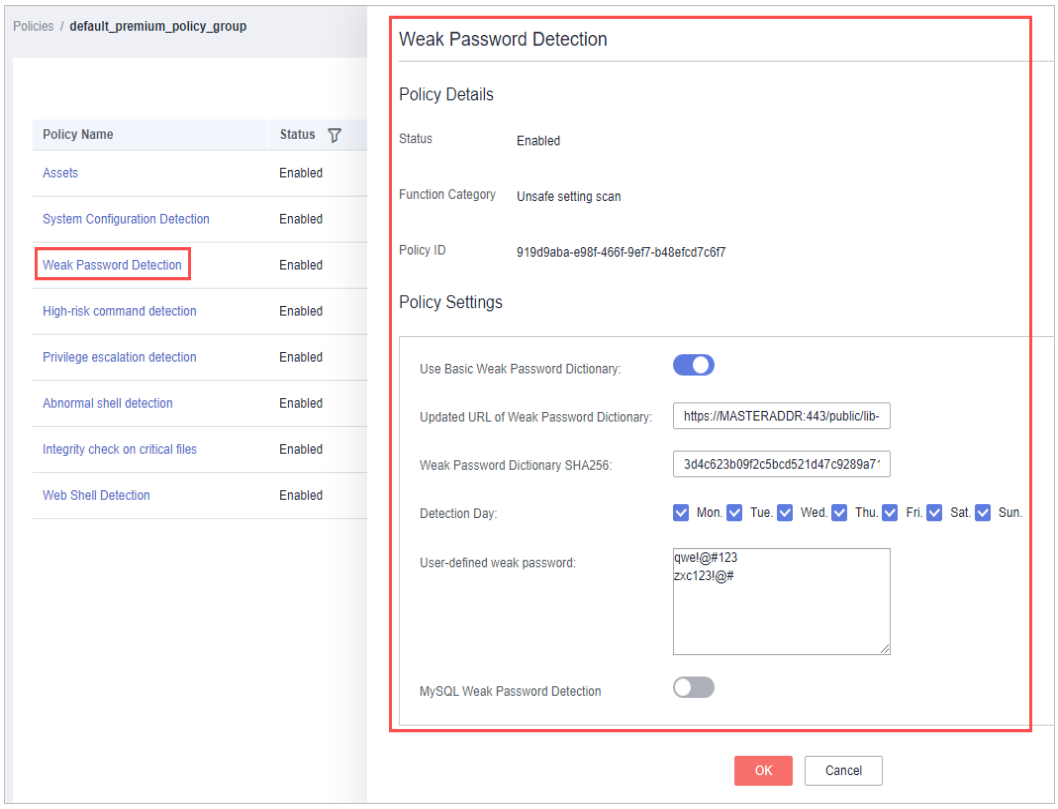


Step 3 Click the name of a policy to check its details. **Figure 10-3** shows the **Weak Password Detection** policy as an example.

NOTE

For details about how to modify a policy, see **Modifying a Policy**.

Figure 10-3 Policy details

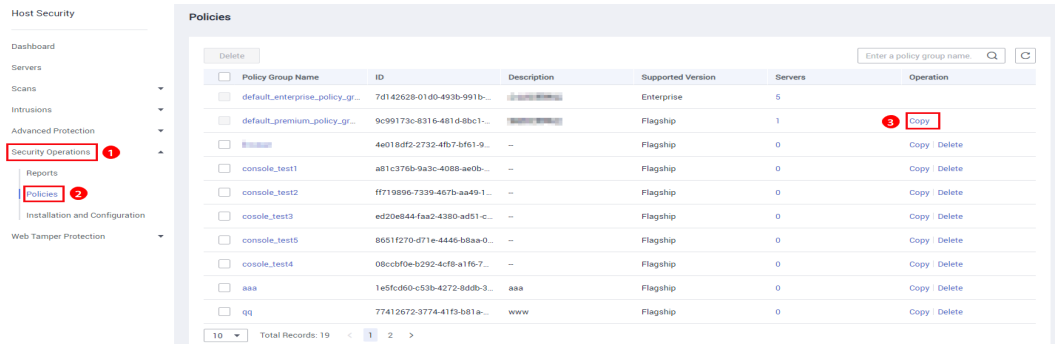


----End

Creating a Policy Group

Step 1 In the row where **default_premium_policy_group (default policy group of the premium edition)** resides, click **Copy** in the **Operation** column, as shown in **Figure 10-4**.

Figure 10-4 Copying a policy group

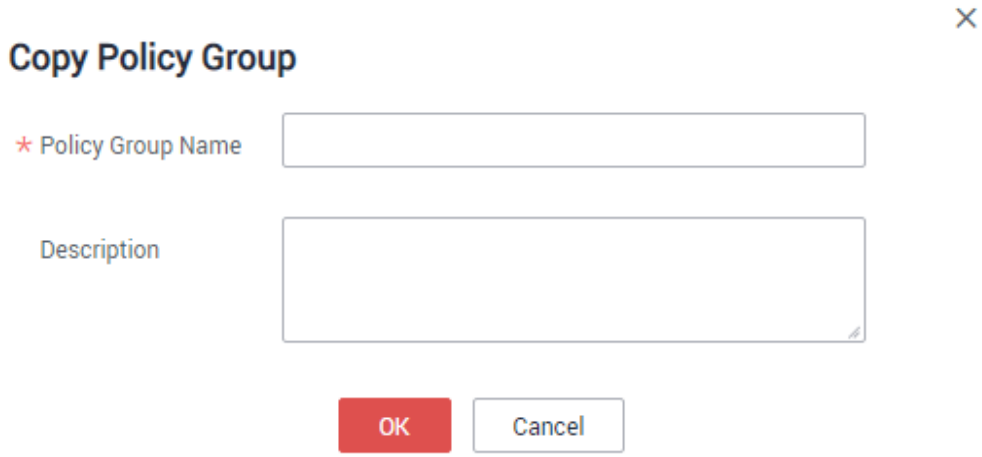


Step 2 In the dialog box displayed, enter a policy group name and description, and click **OK**, as shown in **Figure 10-5**.

NOTE

- 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.

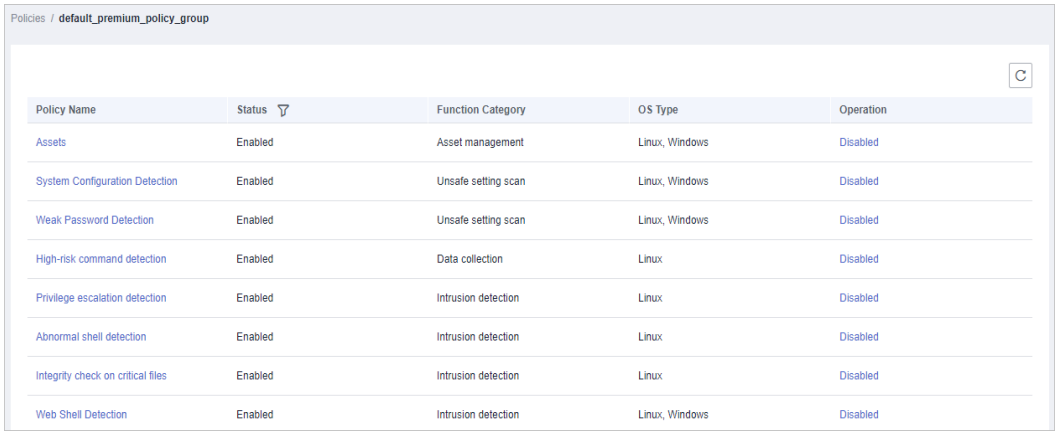
Figure 10-5 Creating a policy group



Step 3 Click **OK**.

Step 4 Click the name of the policy group you just created. The policies in the group will be displayed, as shown in **Figure 10-6**.

Figure 10-6 Policies in a group



Step 5 Click a policy name and modify its settings as required. For details, see **Modifying a Policy**.

Step 6 Enable or disable the policy by clicking the corresponding button in the **Operation** column.

----End

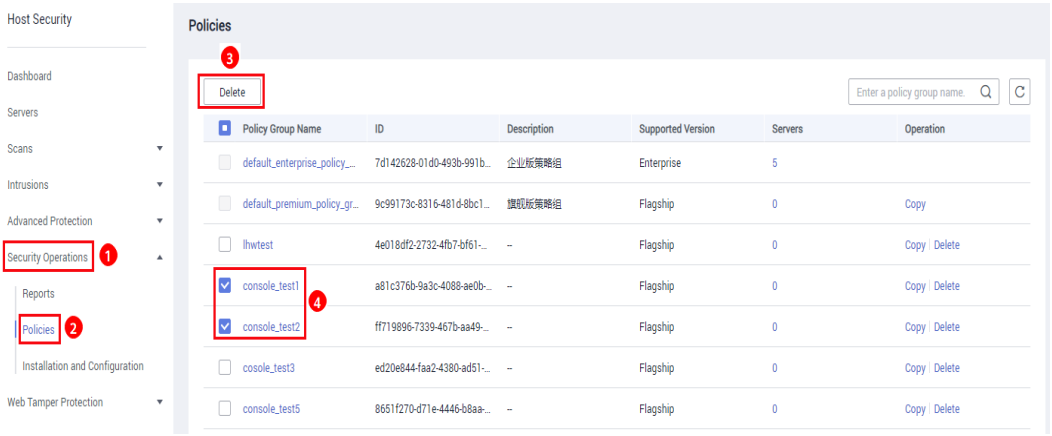
Follow-Up Procedure

Deleting a policy group

After a policy group is deleted, the **Policy Group** column of the servers that were associated with the group will be blank.

Step 1 Select one or more policy groups to be deleted and click **Delete**, as shown in **Figure 10-7**.

Figure 10-7 Deleting policy groups



NOTE

You can also click **Delete** in the **Operation** column of a policy group to delete it.

Step 2 In the displayed dialog box, click **OK**.

----End

10.2 Modifying a Policy

You can modify policies in a policy group.

NOTICE

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** > **Host Security Service**.

Step 3 In the navigation pane, choose **Security Operations** > **Policies**.

----End

Asset

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **Assets**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-8**. For more information, see **Table 10-2**.

Figure 10-8 Assets

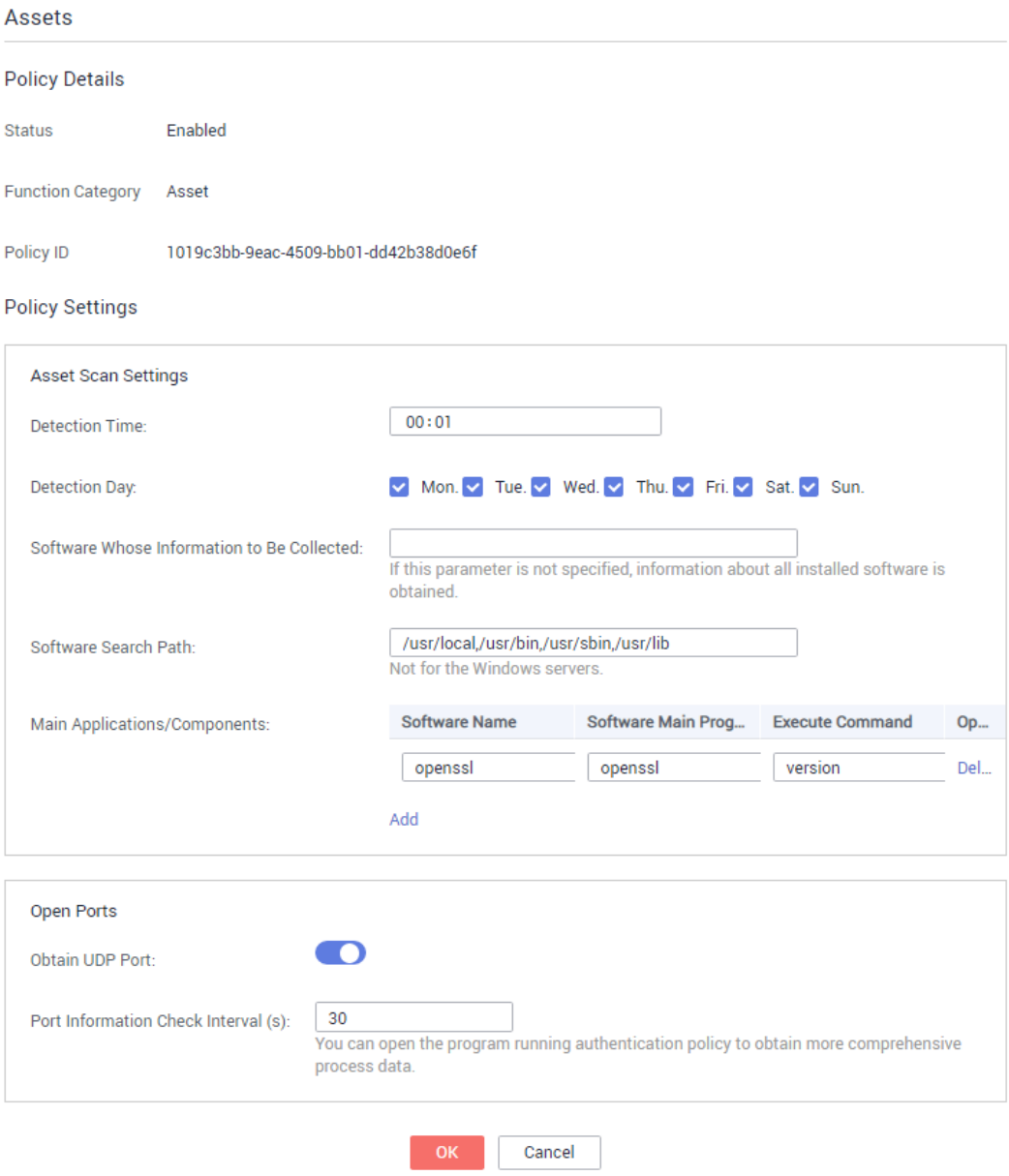


Table 10-2 Assets parameters

Parameter	Description
Detection Time	Time point when scans are performed. It can be accurate to the minute.
Detection Day	Days in a week when assets are scanned. You can select one or more days.

Parameter	Description
Software Whose Information to Be Collected	• Software name. A name can contain a maximum of 5000 characters without any space. Use commas (,) to separate software names. • If this parameter is not specified, information about all installed software will be retrieved as its value.
Software Search Path	Software search path. This parameter is not required for a Windows server.
Main Applications/ Components	• **Software Name** • **Software Main Program** • **Execute Command** • **Operation**: You can click **Add** or **Remove** to modify operations.
Obtain UDP Port	Obtains UDP port information and check the web directories. •  : enable •  : disable
Port Information Check Interval (s)	Interval between two consecutive port checks. The value range is 30s to 86,400s.

Step 4 Click **OK**.

----End

System Configuration Detection

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **System Configuration Detection**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-9**. For more information, see **Table 10-3**.

Figure 10-9 System Configuration Detection

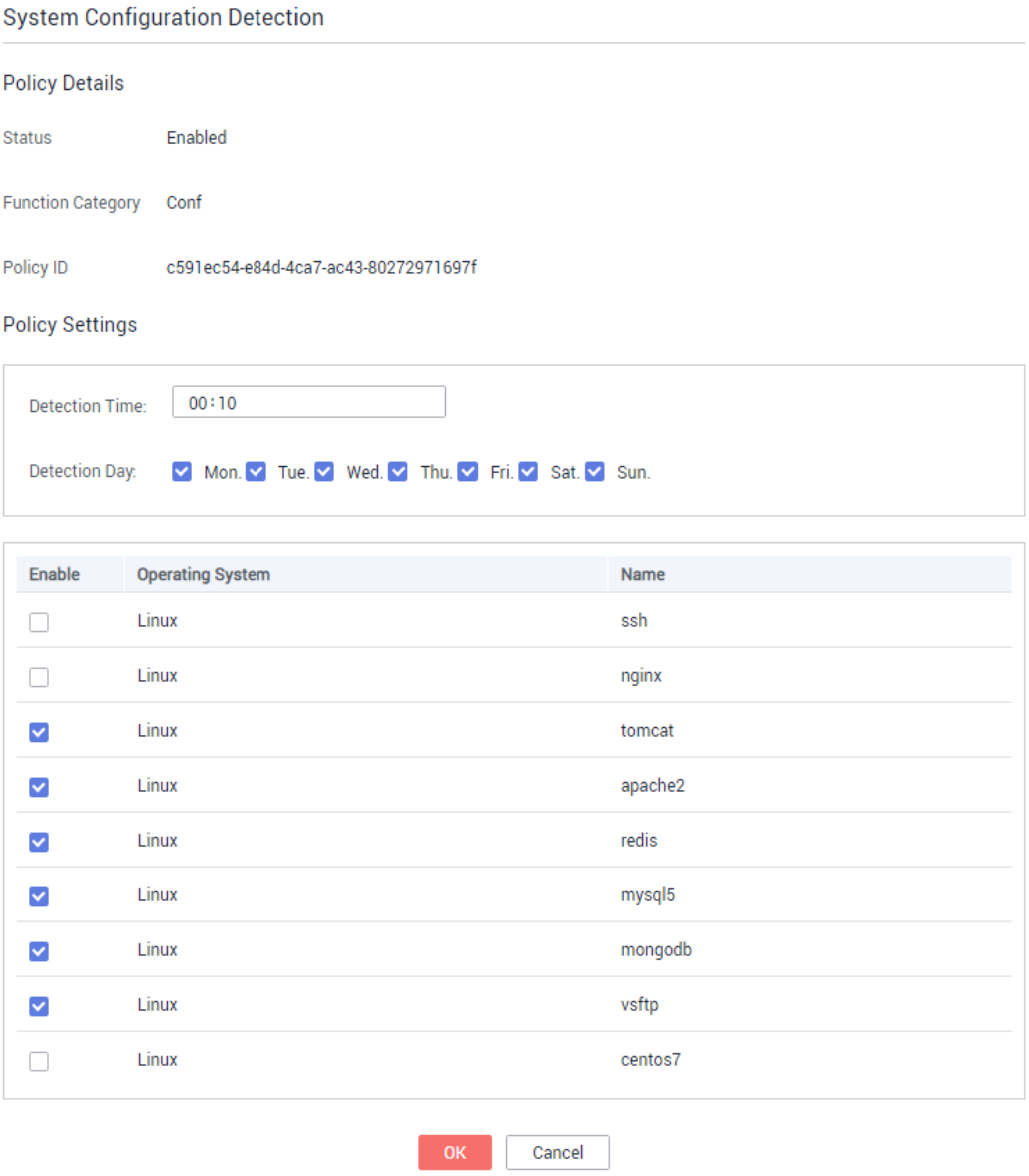


Table 10-3 System configuration detection parameters

Parameter	Description
Detection Time	Time point when detections are performed. It can be accurate to the minute.
Detection Day	Day in a week when a detection is performed. You can select any days from Monday to Sunday.

Step 4 Select the OSs to be checked.

Step 5 Click **OK**.

----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 In the policy group list, click the name of the group that contains the required policy.

Step 2 In the policy group list, click **Weak Password Detection**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-10**. For more information, see **Table 10-4**.

Figure 10-10 Weak password detection

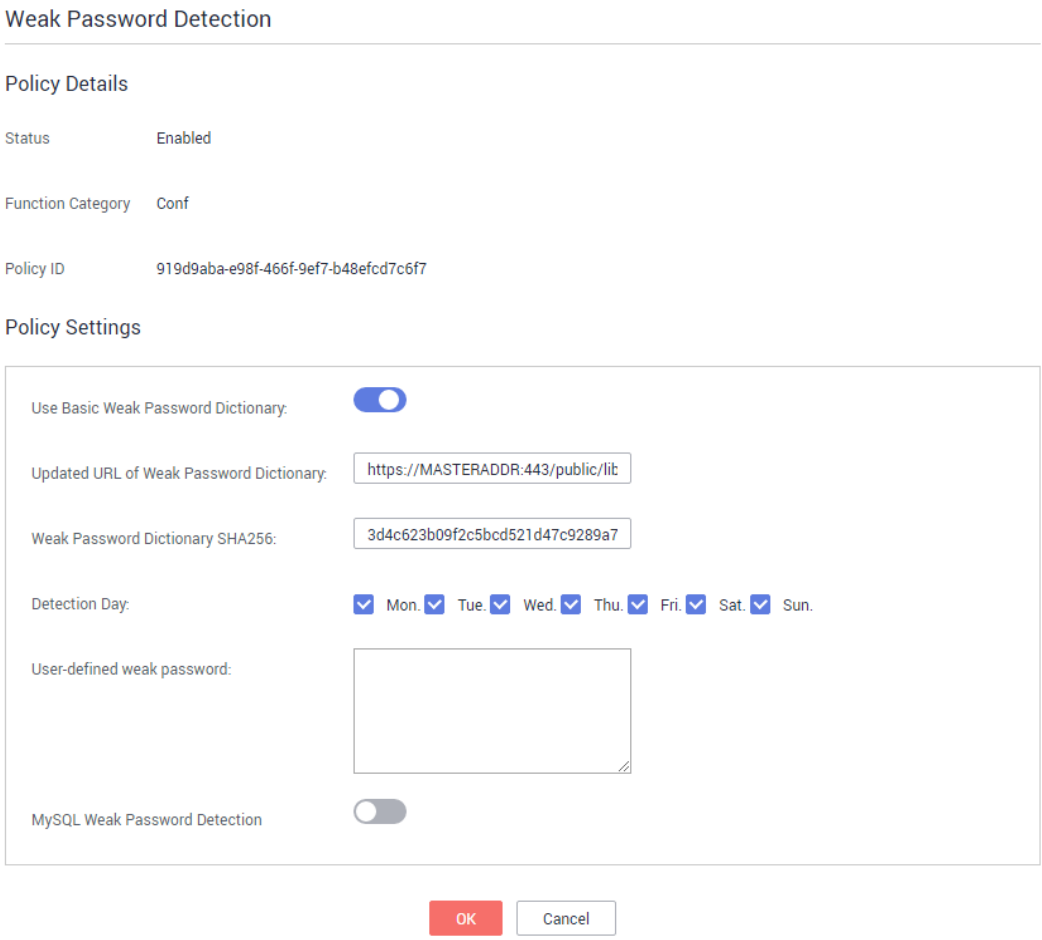


Table 10-4 Weak password detection parameters

Parameter	Description
Use Basic Weak Password Dictionary	Whether to enable the weak password dictionary. •  : enable •  : disable
Updated URL of Weak Password Dictionary	URL of the website that the weak password dictionary gets updates from
Weak Password Dictionary SHA256	SHA256 of the weak password dictionary
Detection Day	Days in a week when weak passwords are scanned. You can select one or more days.
User-defined weak password	You can add a password that may have been leaked to this weak password text box to prevent server accounts from using the password.
MySQL Weak Password Detection	Scans MySQL login passwords for weak passwords.

Step 4 Click **OK**.

----End

High-risk Command Detection

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **High-risk command detection**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-11**. For more information, see **Table 10-5**.

Figure 10-11 High-risk command detection

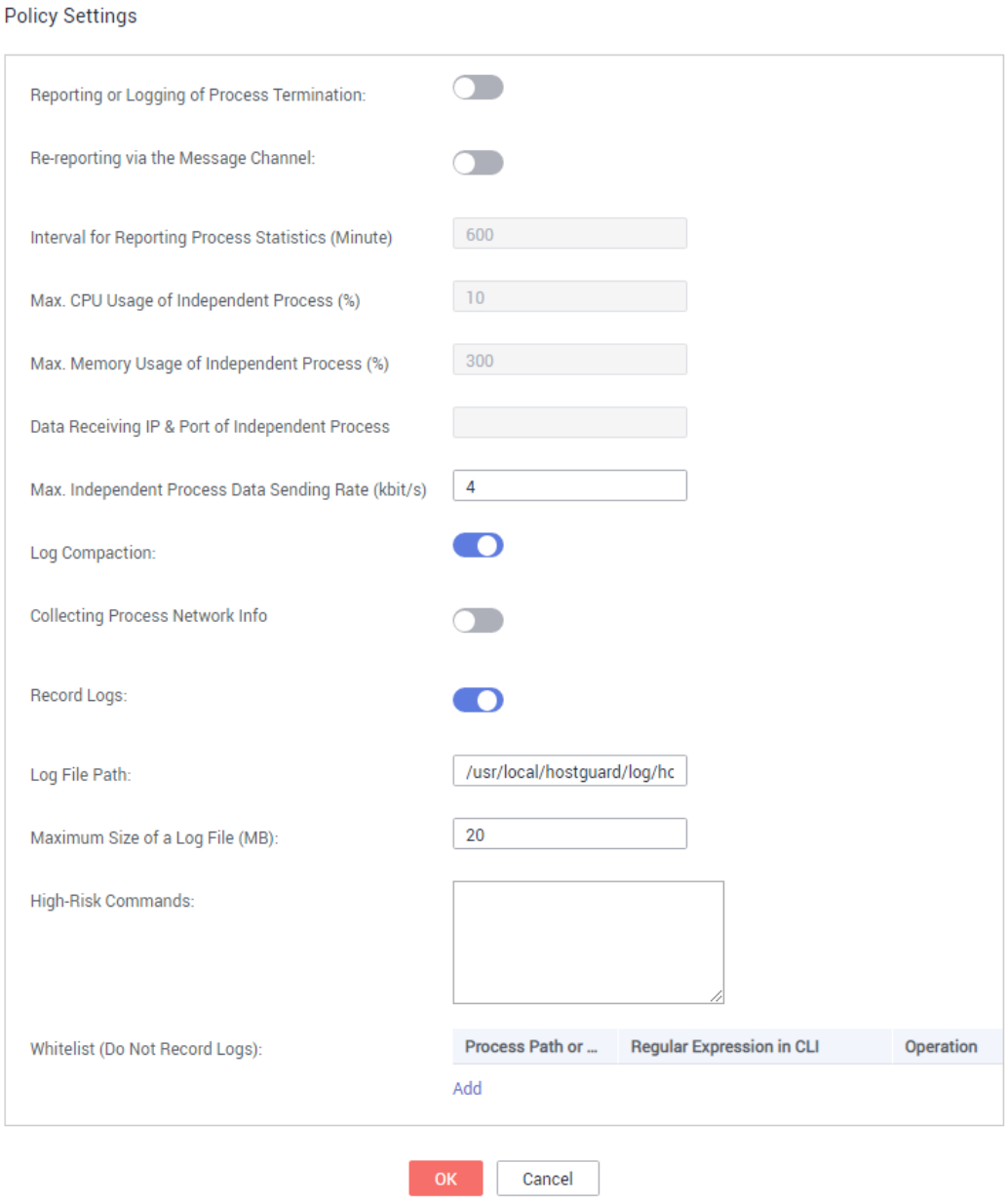


Table 10-5 High-risk command detection parameters

Parameter	Description
Reporting or Logging of Process Termination	Reports or records process termination. • : enable • : disable

Parameter	Description
Re-reporting via the Message Channel	De-duplicates messages reported through the message channel. •  : enable •  : disable
Interval for Reporting Process Statistics (Minute)	This parameter takes effect only if **Re-reporting via the Message Channel** has been enabled. This parameter specifies the interval for reporting process statistics. Set it to a valid number.
Max. CPU usage of Independent Process (%)	This parameter takes effect only if **Re-reporting via the Message Channel** has been enabled. This parameter specifies the maximum CPU usage of an independent process. The value range is 5 to 99.
Max. Memory Usage of Independent Process (MB)	This parameter takes effect only if **Re-reporting via the Message Channel** has been enabled. This parameter specifies the maximum memory usage of an independent process. The value range is 50 to 1024.
Data Receiving IP & Port of Independent Process	This parameter takes effect only if **Re-reporting via the Message Channel** has been enabled. This parameter specifies the data receiving IP address and port of an independent process.
Max. Independent Process Data Sending Rate (kbit/s)	This parameter takes effect only if **Re-reporting via the Message Channel** has been enabled. This parameter specifies the maximum data sending rate of an independent process. The value range is 1 to 100.
Log Compaction	Compacts logs. •  : enable •  : disable
Collecting Process Network Info	Collects network connection information of processes. •  : enable •  : disable
Record Logs	Records logs. •  : enable •  : disable
Log File Path	Log file path

Parameter	Description
Maximum Size of a Log File (MB)	Maximum size of a log file. The value range is 10 to 1024. • If the size of a .log file exceeds the allowed maximum size, the system automatically renames the file as **.log.0**, creates a .log file, and writes logs to the .log file. • There can be a maximum of two log files. If the .log file exceeds the allowed maximum size, the system deletes the **.log.0** file, renames the .log file as **.log.0**, creates a .log file, and writes logs to the .log file.
High-Risk Commands	High-risk commands you want HSS to detect. Each command occupies a line.
Whitelist (Do Not Record Logs)	• **Process Path or Process Name**: full path of a process or full name of a program • **Regular Expression in CLI**: regular expression of a command • **Operation**: You can click **Add** or **Delete** to modify the list of processes and programs.

Step 4 Click **OK**.

----End

Privilege Escalation Detection

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **Privilege escalation detection**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-12**. For more information, see **Table 10-6**.

Figure 10-12 Privilege escalation detection

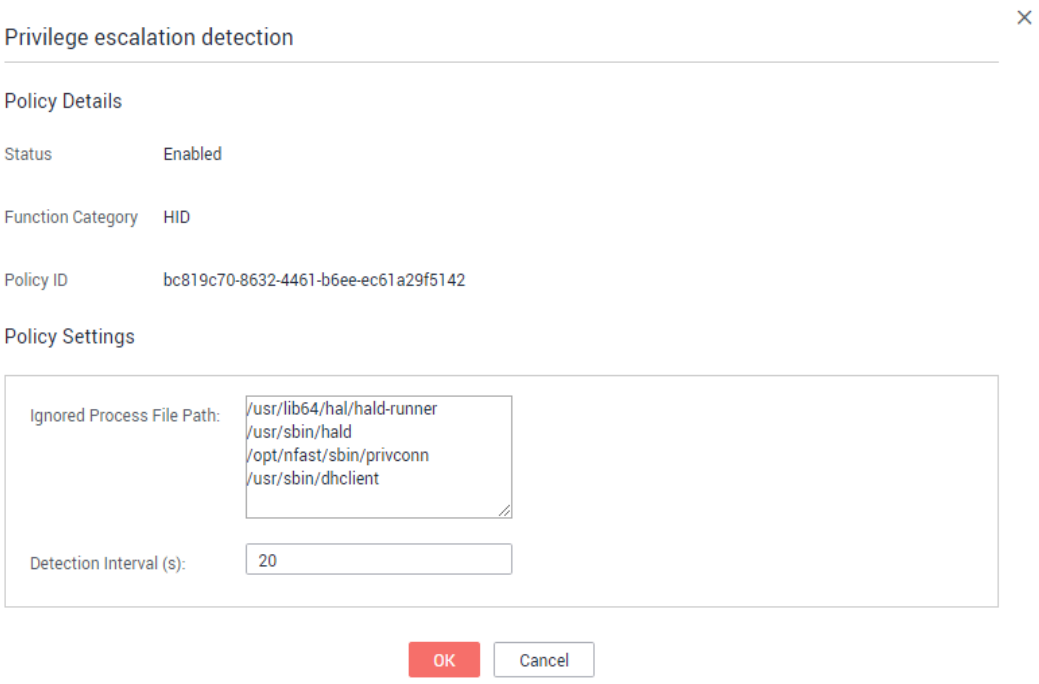


Table 10-6 Privilege escalation detection parameters

Parameter	Description
Ignored Process File Path	Ignored process file path
Detection Interval (s)	Interval for checking process files. The value range is 5 to 3600.

Step 4 Click **OK**.

----End

Abnormal or Reverse Shell Detection

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **Abnormal shell detection**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-13**. For more information, see **Figure 10-13**.

Figure 10-13 Abnormal or reverse shell detection

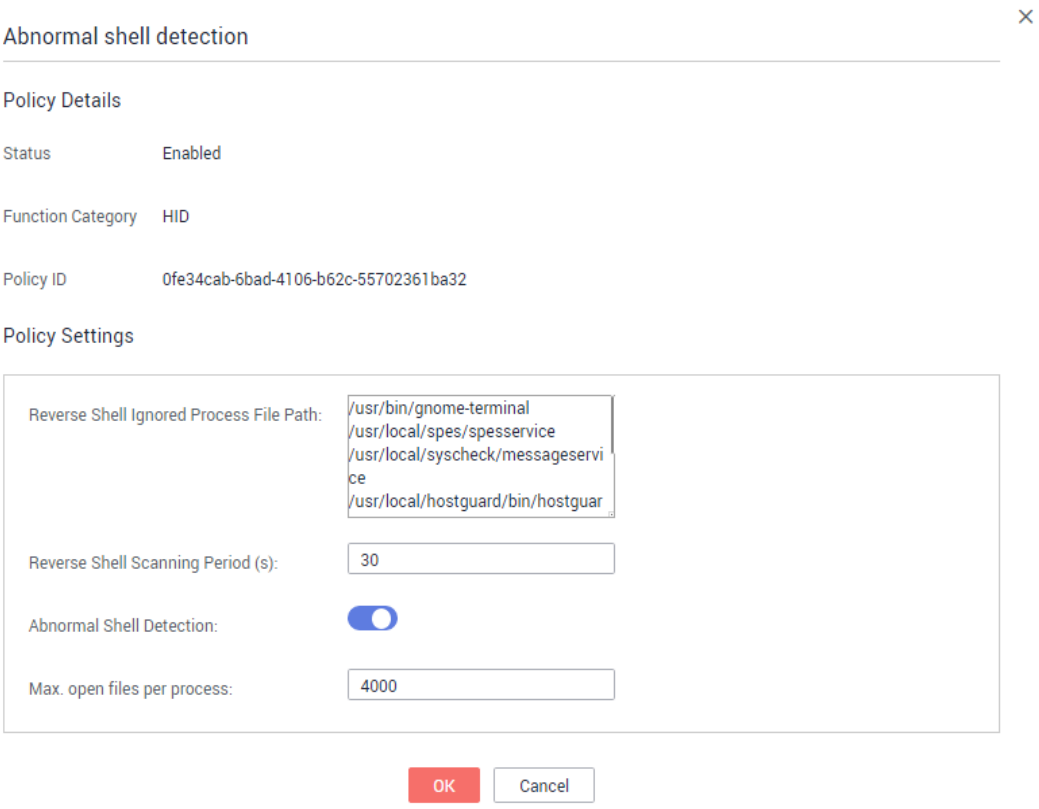


Table 10-7 Abnormal or reverse shell detection parameters

Parameter	Description
Reverse Shell Ignored Process File Path	Process file path to be ignored in reverse shell detection
Reverse Shell Scanning Period (s):	Reverse shell scanning period. The value range is 30 to 86,400.
Abnormal Shell Detection	Detects abnormal shells. You are advised to enable it. • : enable • : disable
Max. open files per process	Maximum number of files that can be opened by a process. The value range is 10 to 300,000.

Step 4 Click **OK**.

----End

File Integrity Monitoring

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **Integrity check on critical files**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-14**. For more information, see **Table 10-8**.

Figure 10-14 Integrity check on critical files

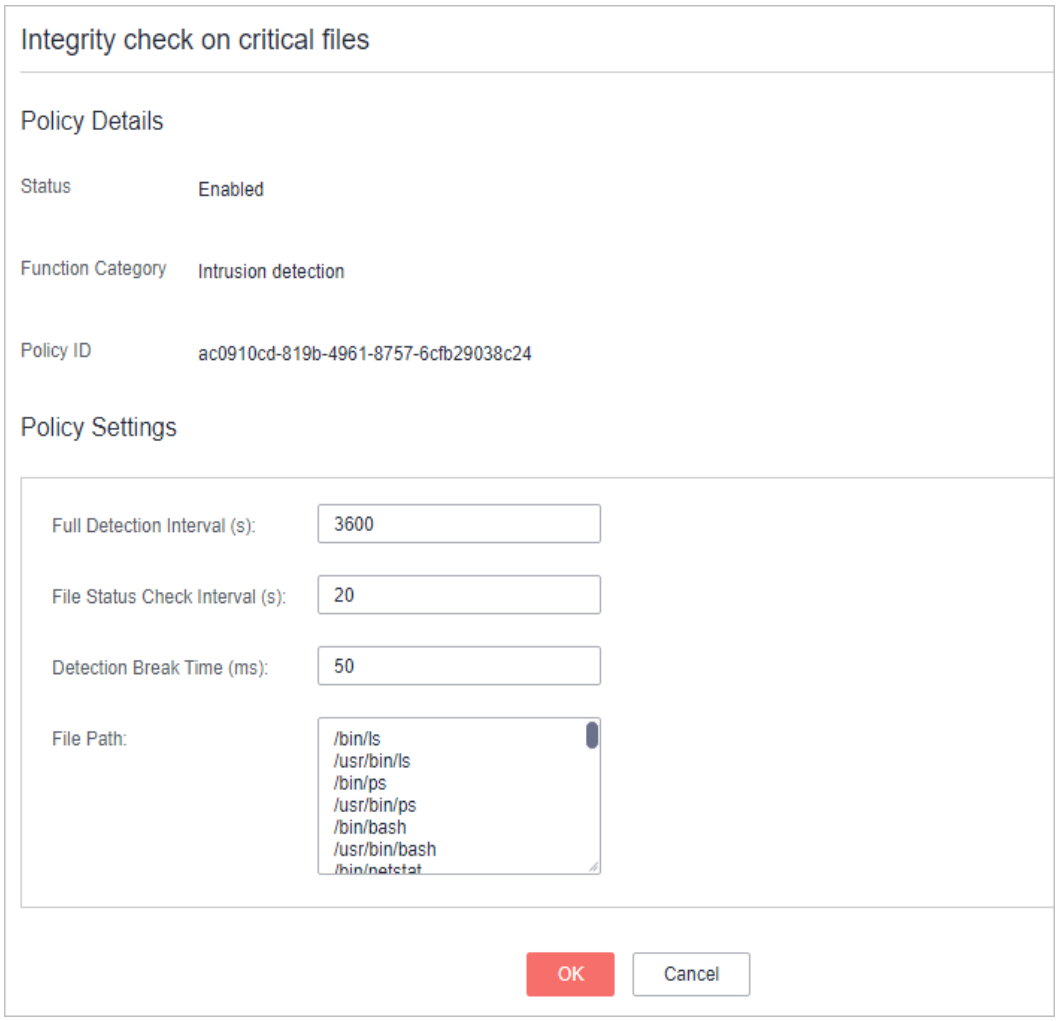


Table 10-8 File integrity monitoring parameters

Parameter	Description
Full Detection Interval (s)	Interval between two consecutive full scans on specified files. The value range is 3,600 to 100,000. For example, setting it to **3600** means the full scan is performed every hour.
File Status Check Interval (s)	Interval for checking file status. The value range is 10 to 600.

Parameter	Description
Detection Break Time (ms)	Interval between the checks of two files. The value range is 0 to 1000. For example, if this parameter is set to **50**, the system checks **/usr/bin/ls** 50 milliseconds after it checks **/bin/ls**.
File Path	Path of the files to be checked **NOTE** • Exercise caution when modifying its settings. Its default values are all critical files and you are not advised to delete any of them. • HSS does not monitor changes on the files that are not specified here.

Step 4 Click **OK**.

----End

Web Shell Detection

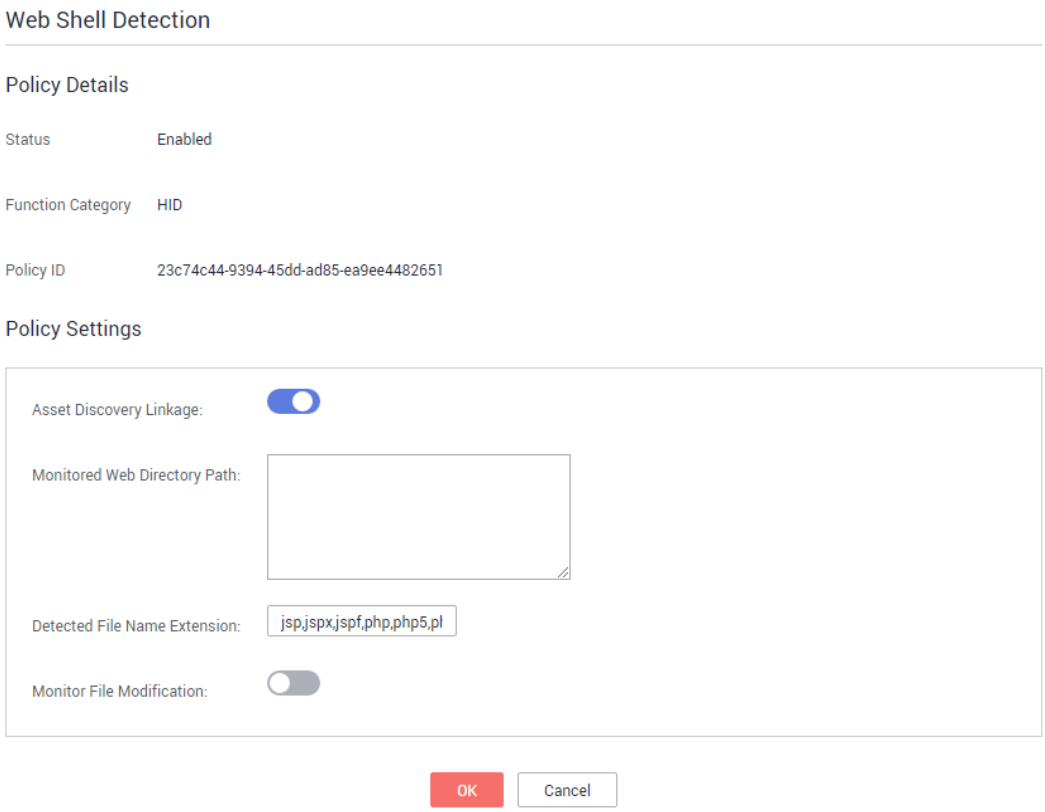
Web shell detection takes effect only after a web path is set.

Step 1 In the policy group list, click the name of the group that contains the required policy.

Step 2 Click **Web Shell Detection**.

Step 3 In the **Policy Settings** area, modify the settings as required, as shown in **Figure 10-15**. For more information, see **Table 10-9**.

Figure 10-15 Web shell detection



NOTE

To prevent the software in web paths from affecting the HSS agent, do not set web paths under **/usr/local**.

Table 10-9 Web shell detection parameters

Parameter	Description
Asset Discovery Linkage	Automatically scans the web paths you specified. • : enable • : disable
Monitored Web Directory Path	Web paths to be scanned. A file path must: • Start with a slash (/) and end with no slashes (/). • End with a port number. • Occupy a separate line and cannot contain spaces.
Detected File Name Extension	Extensions of files to be checked. Valid values include **jsp**, **jspx**, **jspf**, **php**, **php5**, **php4**.
Monitor File Modification	Monitors modifications on files.

Step 4 Click **OK**.

----End

11 WTP

11.1 Adding a Protected Directory or File System

WTP monitors website directories in real time, backs up files, and restores tampered files using the backup, protecting websites from Trojan horses, illegal links, and tampering.

You can specify **directories** or **network file systems** to protect.

Constraints and Limitations

WTP only protects files in the protected directories you set. It does not protect the files specified by the links in protected files.

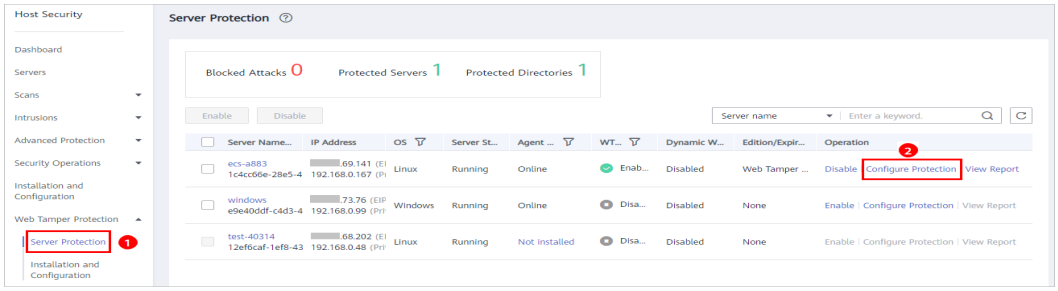
Setting a Protected Directory

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** > **Host Security Service**.

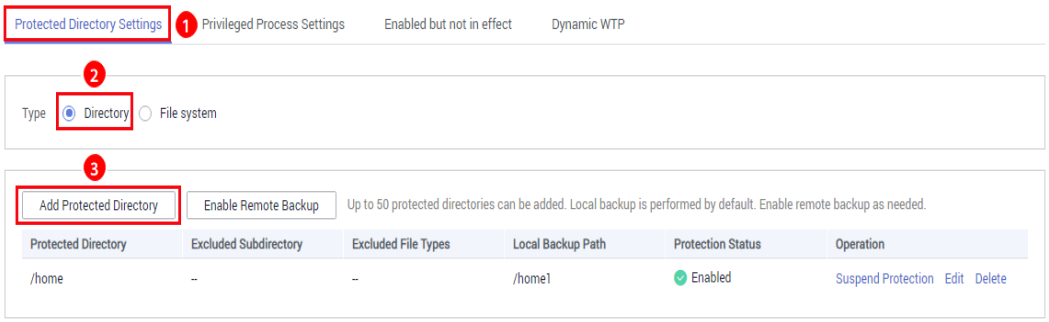
Step 3 Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-1 Web Tamper Protection page



Step 4 Set **Type** to **Directory**.

Figure 11-2 Setting a protected directory



Step 5 You can add a maximum of 50 protected directories.

1. Click **Add**. In the **Add Protected Directory** dialog box, set required parameters. For details, see **Table 11-1**.

Figure 11-3 Adding a protected directory

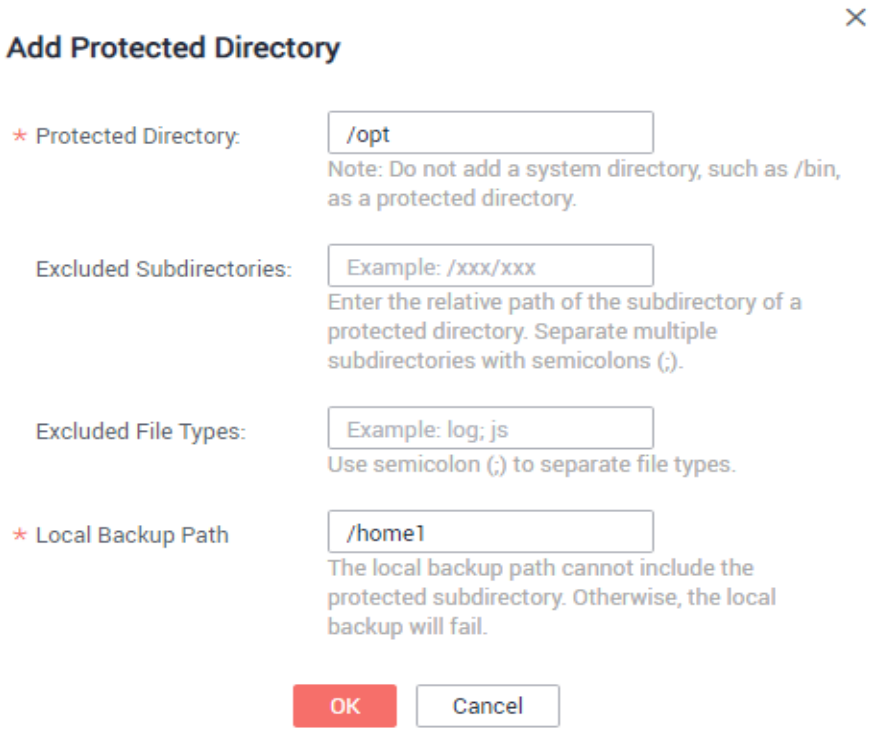


Table 11-1 Parameters for a protected directory

Parameter	Description	Restriction
Protected Directory	Files and folders in this directory are read-only.	Do not set it to any OS directories.

Parameter	Description	Restriction
Excluded Subdirectories	Subdirectories that do not need to be protected in the protected directory, such as temporary file directories. Separate subdirectories with semicolons (;).	The subdirectory is a relative directory in the protected directory.
Excluded File Types	Types of files that do not need to be protected in the protected directory, such as log files. Separate file types with semicolons (;). To record the running status of the server in real time, exclude the log files in the protected directory. You can grant high read and write permissions for log files to prevent attackers from viewing or tampering with the log files.	-
Local Backup Path	After WTP is enabled, files in the protected directory are automatically backed up to the local backup path. Generally, the backup completes within 10 minutes. The actual duration depends on the size of files in the protected directory. Protection takes effect immediately when the backup completes. Excluded subdirectories and types of files are not backed up. If WTP detects that a file in a protected directory is tampered with, it immediately uses the backup file on the local server to restore the file.	The local backup path cannot overlap with the added protected directory.

2. Click **OK**.

   If you need to modify files in the protected directory, stop protection for the protected directory first. After the files are modified, resume protection for the directory in a timely manner.

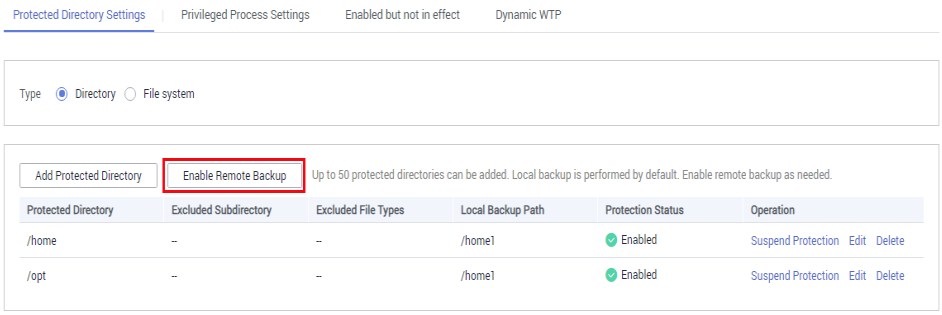
Step 6 Enable remote backup.

By default, HSS backs up the files from the protected directories (excluding specified subdirectories and file types) to the local backup directory you specified when adding protected directories. To protect the local backup files from tampering, you must enable the remote backup function.

For details about how to add a remote backup server, see **Adding a Remote Backup Server**.

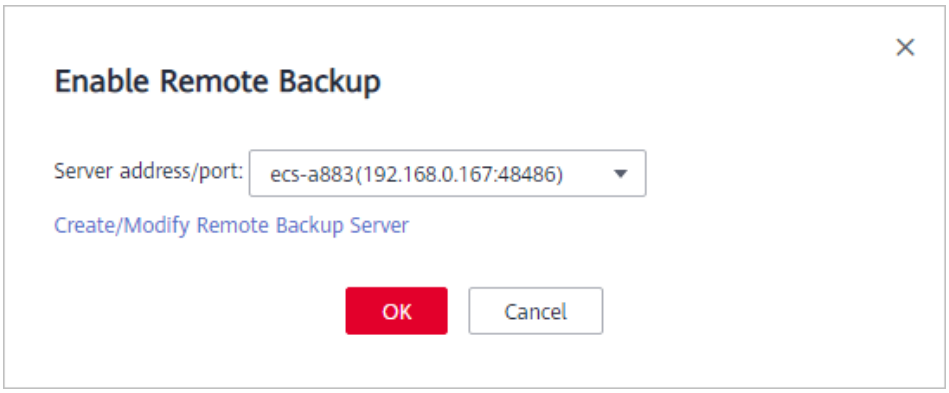
1. Click **Enable Remote Backup**.

   Figure 11-4 Enabling remote backup

2. Select a backup server from the drop-down list box.

   Figure 11-5 Setting remote backup

3. Click **OK**.

----End

Setting a Protected File System

NOTE

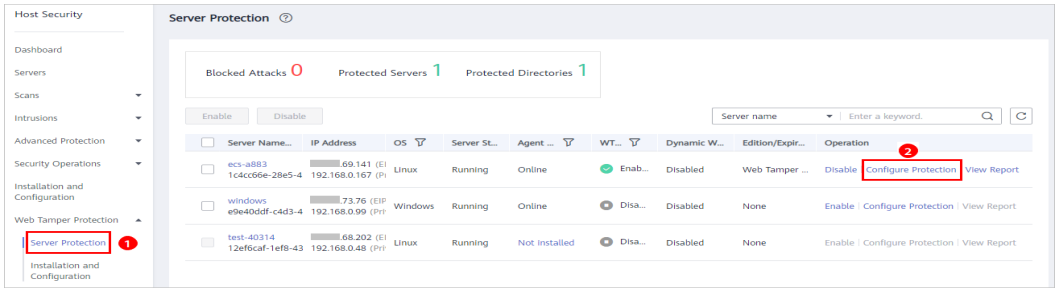
Only network file systems running the Linux OS can be protected.

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** > **Host Security Service**.

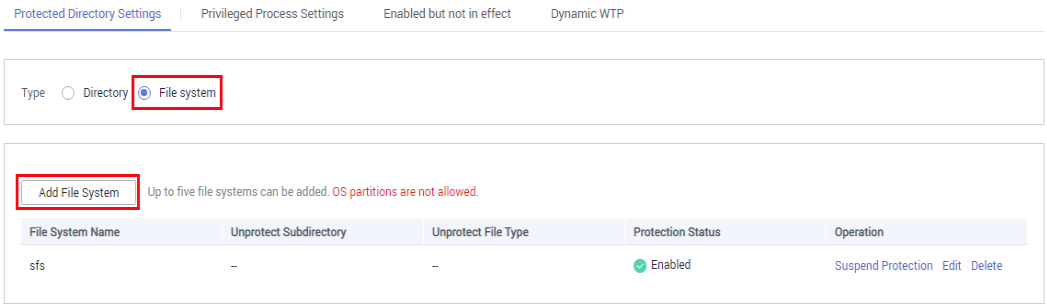
Step 3 Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-6 Web Tamper Protection page



Step 4 Set **Type** to **File system**.

Figure 11-7 Setting a protected file system



Step 5 Click **Add File System**. In the **Add Protected Directory** dialog box, set required parameters. For details, see **Table 11-2**.

Figure 11-8 Adding a file system

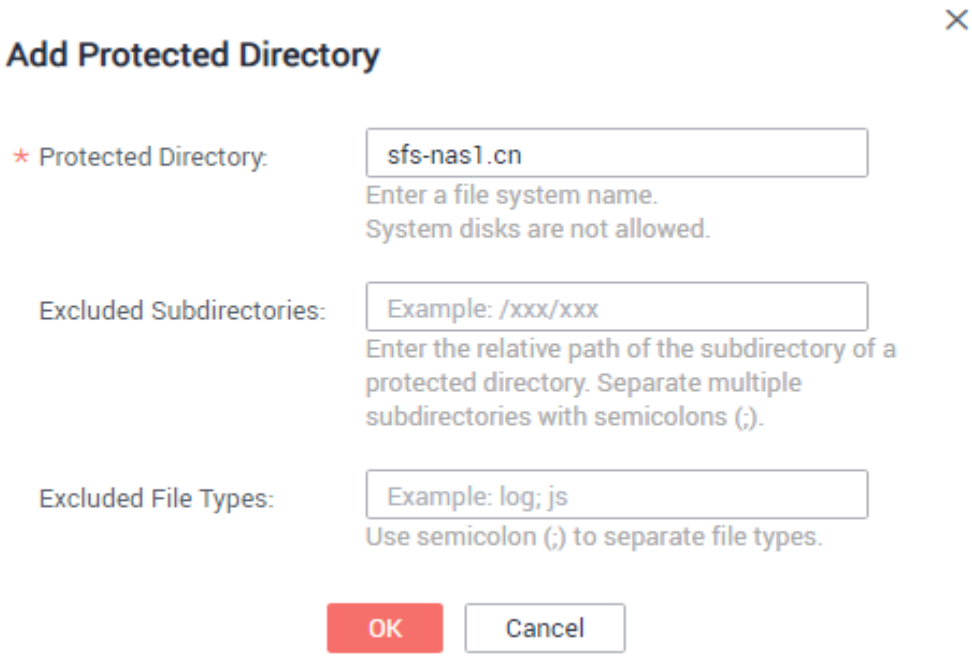
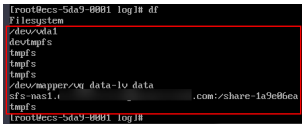


Table 11-2 Parameters for a protected directory

Parameter	Description	Restriction
File System	Files and directories in the protected file system are read-only. **NOTE** Run the **df** command to view all file systems. As shown in the following figure, the **Filesystem** column indicates the file system name. **Figure 11-9** File system 	Do not set it to any system disks.
Excluded Subdirectories	Subdirectories that do not need to be protected in the protected file system, such as temporary file directories. Separate subdirectories with semicolons (;).	The subdirectory is a relative directory in the file system.
Excluded File Types	Types of files that do not need to be protected in the protected file system, such as log files. Separate file types with semicolons (;).	-

NOTICE

You can **set privileged processes** that can modify files in protected directories. Ensure that the privileged processes are secure and reliable.

Step 6 Click **OK**.

----End

Follow-Up Procedure

- Suspend protection: You can suspend WTP for a directory if needed. It is best practice that you resume WTP in a timely manner to prevent the files in the directory from being tampered with.
- Edit a protected directory: You can modify the added protected directory as needed.

- Delete a protected directory: You can delete the directories that do not need to be protected.

NOTICE

- After you suspend protection for a protected directory, delete it, or modify its path, files in the directory will no longer be protected. Before performing these operations, ensure you have taken other measures to protect the files.
- After you suspend protection for a protected directory, delete it, or modify its path, if you find your files missing in the directory, search for them in the local or remote backup path.

11.2 Adding a Remote Backup Server

By default, HSS backs up the files from the protected directories (excluding specified subdirectories and file types) to the local backup directory you specified when adding protected directories. To protect the local backup files from tampering, you must enable the remote backup function.

If a file directory or backup directory on the local server becomes invalid, you can use the remote backup service to restore the tampered web page.

Prerequisites

The following servers can be used as remote backup servers:

Linux servers whose **Server Status** is **Running** and **Agent Status** is **Online**

NOTICE

- The remote backup function can be used when the Linux backup server is connected to your cloud server. To ensure a proper backup, you are advised to select a backup server on the same intranet as your cloud server.
- You are advised to use intranet servers least exposed to attacks as the remote backup servers.

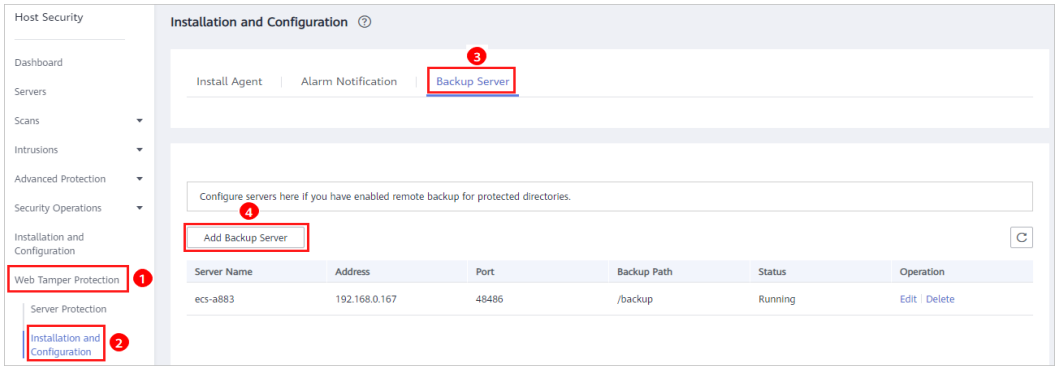
Configuring a Remote Backup Server

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** > **Host Security Service**.

Step 3 Choose **Web Tamper Protection** > **Installation and Configuration**. Click the **Backup Server** tab and click **Add Backup Server**.

Figure 11-10 Configuring a backup server



Step 4 In the displayed dialog box, add a remote backup server and set required parameters. For details, see **Table 11-3**.

Figure 11-11 Adding a remote backup server

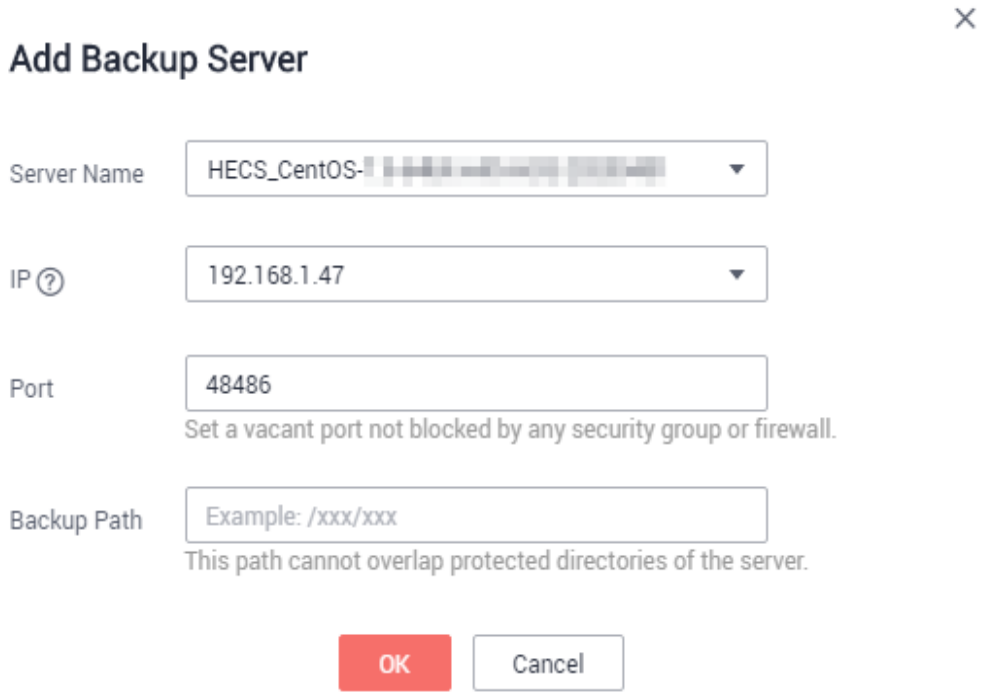


Table 11-3 Parameters for a remote backup server

Parameter	Description
Address	This address is the private network address of the server.
Port	Ensure that the port is not blocked by any security group or firewall or occupied.

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

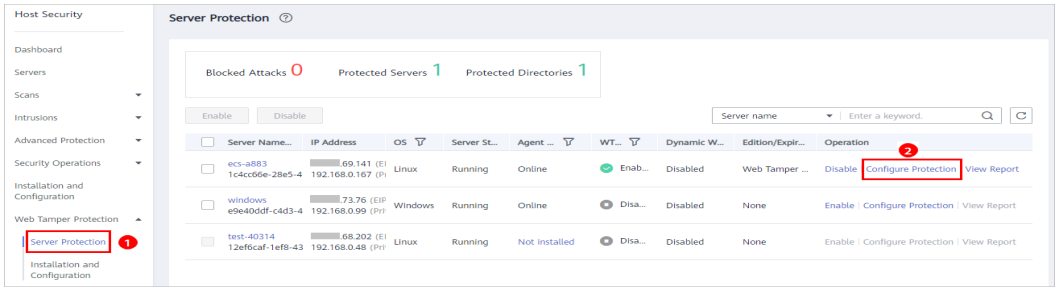
Step 5 Click **OK**.

----End

Enabling Remote Backup

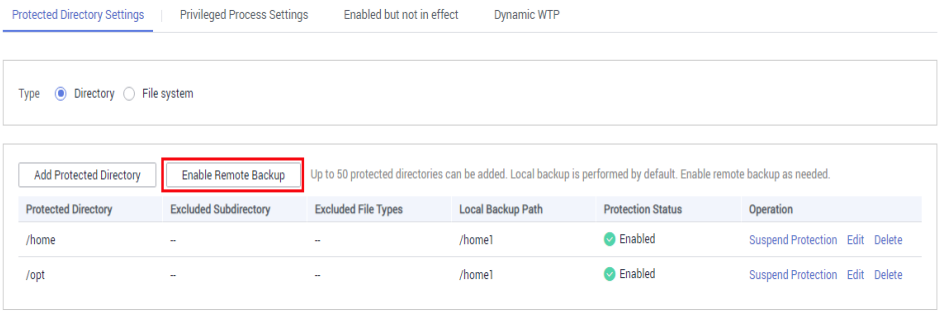
Step 1 Choose **Web Tamper Protection** > **Server Protection**. Click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-12 Web Tamper Protection page



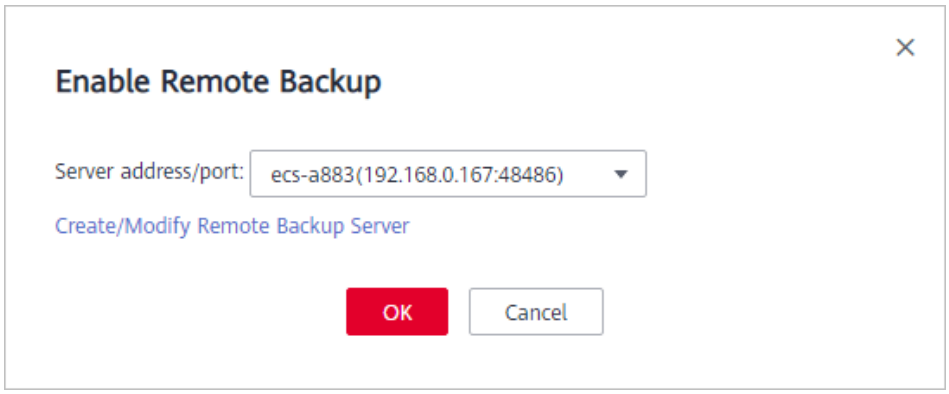
Step 2 Set **Type** to **Directory** and click **Enable Remote Backup**.

Figure 11-13 Enabling remote backup



Step 3 In the **Enable Remote Backup** drop-down list, select a server.

Figure 11-14 Setting remote backup



Step 4 Click **OK**.

----End

Follow-Up Procedure

Disabling remote backup

Exercise caution when performing this operation. If remote backup is disabled, HSS will no longer back up files in your protected directories.

11.3 Adding a Privileged Process That Can Modify Protected Files

After WTP is enabled, the content in the protected directories is read-only. To allow certain processes to modify files in the directories, you can add them to the privileged process list.

Only the modification made by privileged processes can take effect. Modifications made by other processes will be automatically rolled back.

Exercise caution when adding privileged processes. Do not let untrustworthy processes access your protected directories.

A maximum of 10 process file paths can be added to each server.

Prerequisites

- On the **Server Protection** page of the WTP console, the **Agent Status** of the target server is **Online**, and the **Protection Status** of the server is **Enabled**.
- For Linux a server, you have set **Type** to **File system** on the **Protected Directory Settings** tab. To open the tab, choose **Web Tamper Protection** > **Server Protection**, and click **Configure Protection** in the **Operation** column of the required server.

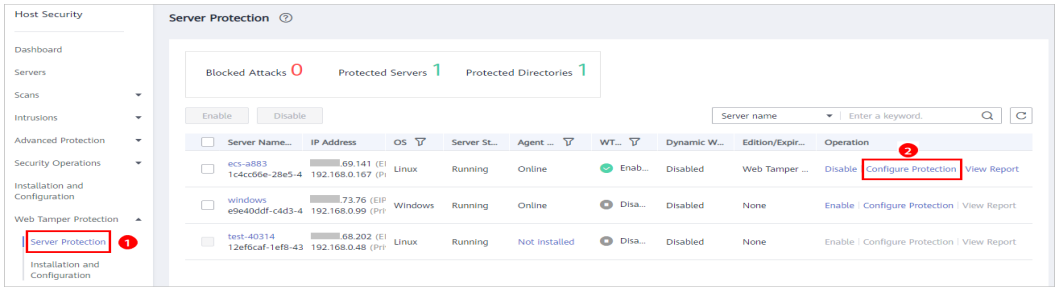
Adding a Privileged Process

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** > **Host Security Service**.

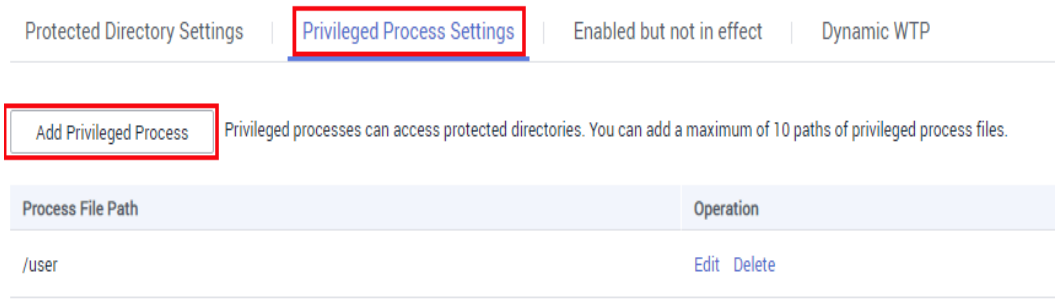
Step 3 Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-15 Web Tamper Protection page



Step 4 On the **Privileged Process Settings** tab, click **Add Privileged Process**.

Figure 11-16 Adding a privileged process



Step 5 In the **Add Privileged Process** dialog box, enter the path of the privileged process.

The process file path must contain the process name and extension, for example, **C:/Path/Software.type**. If the process has no extension, ensure the process name is unique.

Step 6 Click **OK**.

----End

Follow-Up Procedure

Modifying or deleting existing privileged processes

In the **Operation** column of a process file path, click **Edit** to modify the privileged processes or click **Delete** to delete it if it is unnecessary.

NOTE

- After you edit or delete the process file path, the privileged process cannot modify the files in the protected directory. To avoid impact on services, exercise caution when performing these operations.
- Unnecessary processes may be exploited by attackers due to process vulnerabilities. Therefore, delete unnecessary privileged processes in a timely manner.

11.4 Setting Scheduled WTP Protection

You can schedule WTP protection to allow website updates in specific periods.

NOTE

Exercise caution when you set the periods to disable WTP, because files will not be protected in those periods.

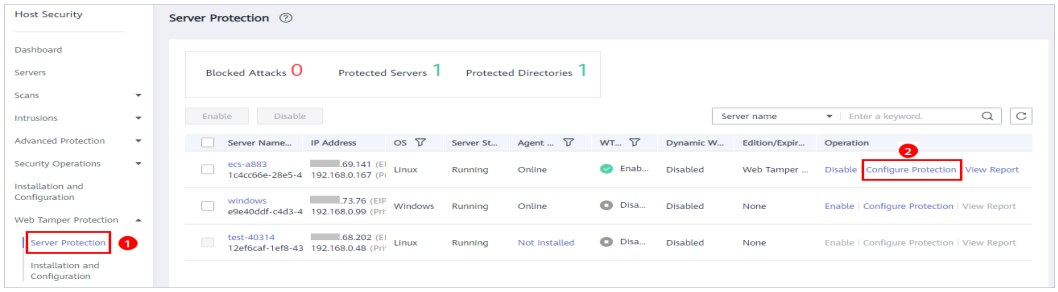
Procedure

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** > **Host Security Service**.

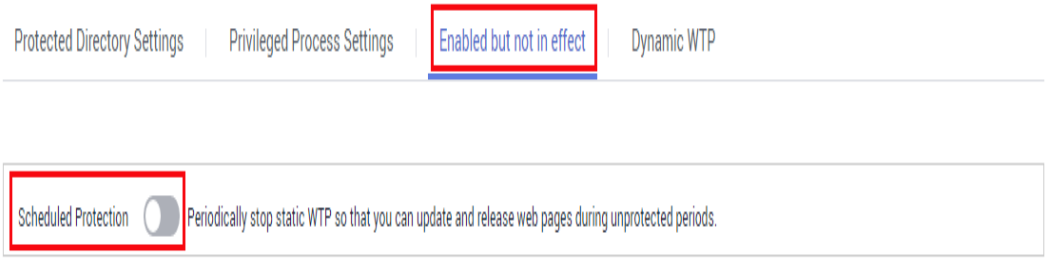
Step 3 Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-17 Web Tamper Protection page



Step 4 Enable scheduled protection.

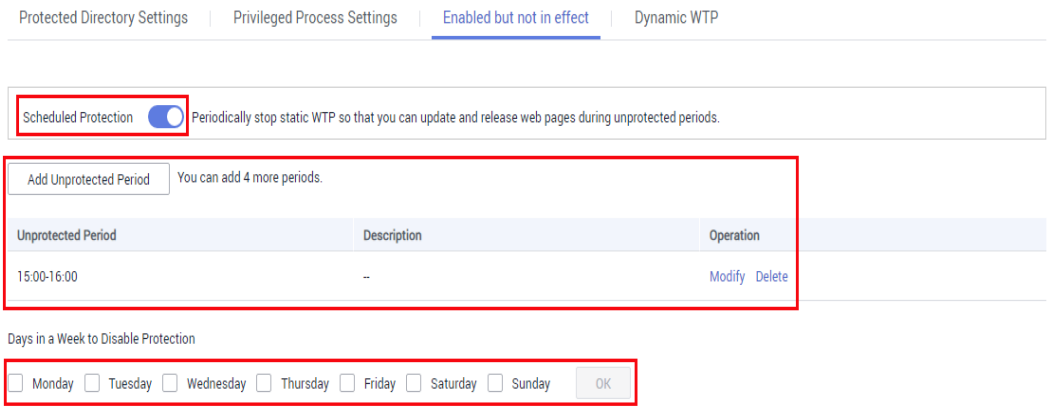
Figure 11-18 Scheduled protection



Step 5 Click **OK**.

Step 6 Set **Unprotected Period** and **Days in a Week to Disable Protection**.

Figure 11-19 Setting scheduled protection parameters



----End

Rules for Setting an Unprotected Period

- Unprotected period >= 5 minutes
- Unprotected period < 24 hours
- Periods (except for those starting at 00:00 or ending at 23:59) cannot overlap and must have an at least 5-minute interval.
- A period cannot span two days.
- The server time is used as a time base.

11.5 Enabling Dynamic WTP

Dynamic WTP protects your web pages while Tomcat applications are running, and can detect tampering of dynamic data, such as database data. It can be enabled with static WTP or separately.

Prerequisites

You are using a server running the Linux OS.

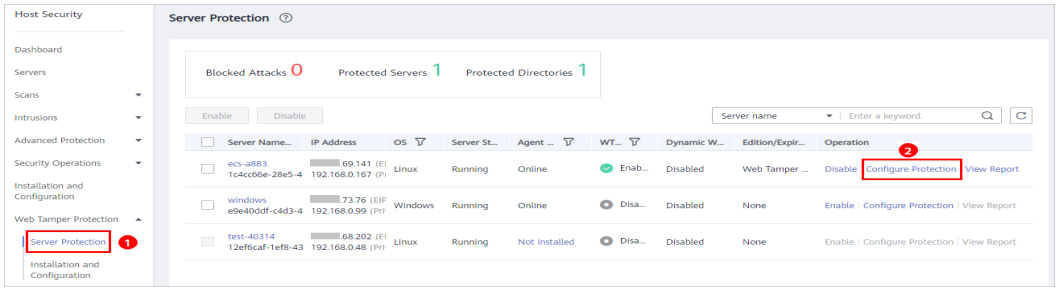
Procedure

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** > **Host Security Service**.

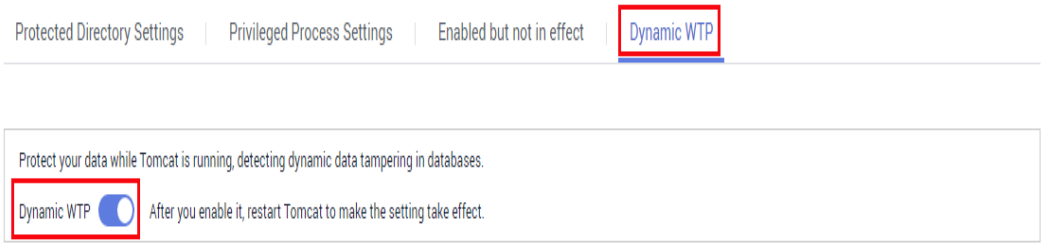
Step 3 Choose **Web Tamper Protection** > **Server Protection**, click **Configure Protection**. The **Protected Directory Settings** tab is displayed.

Figure 11-20 Web Tamper Protection page



Step 4 Click the **Dynamic WTP** tab and enable the function.

Figure 11-21 Dynamic WTP



Step 5 Restart Tomcat for the function to take effect.

----End

11.6 Viewing WTP Reports

Once WTP is enabled, the HSS service will comprehensively check protected directories you specified. You can check records about detected tampering attacks.

Prerequisites

- Login credentials have been obtained.
- **Agent Status** of the server is **Online**, and its **WTP Status** is **Enabled**.

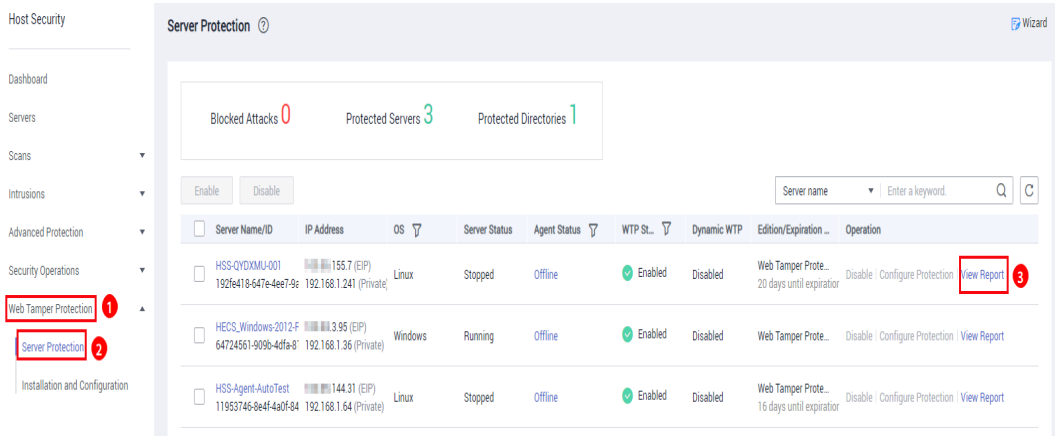
Procedure

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** > **Host Security Service**.

Step 3 On the WTP console, Choose **Server Protection**. Click **View Report** in the **Operation** column.

Figure 11-22 Viewing a protection record



Step 4 View details on the report page.

Figure 11-23 Static WTP records

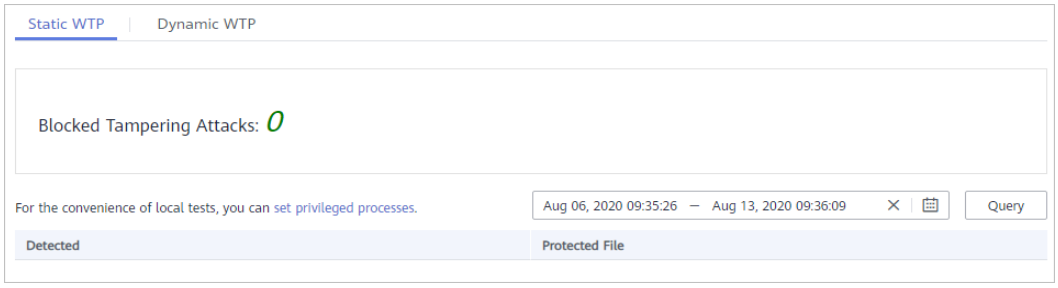
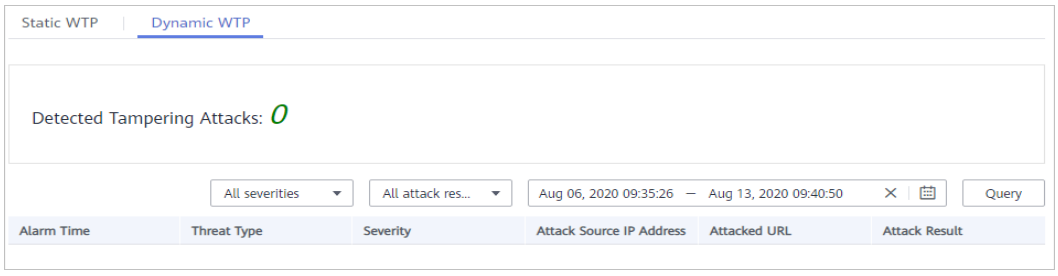


Figure 11-24 Dynamic WTP records



----End

12 Audit

12.1 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 12-1 lists HSS operations recorded by CTS.

Table 12-1 HSS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Enabling HSS	hss	openHssProtect
Disabling HSS	hss	closeHssProtect
Starting a manual detection	hss	manualDetection
Unblocking an IP address	hss	unblockIp
Configuring common login locations	hss	setCommonLocation
Configuring a login IP address whitelist	hss	setWhiteIpList
Enabling or disabling a login IP address whitelist	hss	switchWhiteIpList
Ignoring a port	hss	ignorePort
Unignoring a port	hss	noIgnorePort
Ignoring a risky configuration	hss	ignoreConfigRisky
Unignoring a risky configuration	hss	notIgnoreConfigRisky
One-click vulnerability fix	hss	repairVul

Operation	Resource Type	Trace Name
Verifying a vulnerability	hss	verifyVul
Waiting for system restart and verification after one-click fix	hss	confirmVul
Ignoring a software vulnerability	hss	ignoreVul
Unignoring a software vulnerability	hss	notIgnoreVul
Enabling a firewall	HSS	turnonFirewall
Enabling WTP	HSS	openWtp
Disabling WTP	hss	stopWtp
Adding a protected directory to WTP	hss	addWtpDir
Removing a protected directory from WTP	hss	deleteWtpDir
Changing a protected directory in WTP	hss	modifyWtpDir
Suspending protection for a protected directory in WTP	hss	suspendWtpDir
Resuming protection for a protected directory in WTP	hss	resumeWtpDir
Setting a backup server for WTP	hss	setWtpBackupHost
Setting remote backup for WTP	hss	setWtpRemoteBackup
Adding a privileged process in WTP	hss	addWtpPrivilegedProcess
Removing a privileged process from WTP	hss	deleteWtpPrivilegedProcess
Modifying a privileged process in WTP	hss	modifyWtpPrivilegedProcess
Enabling two-factor authentication	hss	turnOnTwoFactor
Disabling two-factor authentication	hss	turnOffTwoFactor
Changing the topic for two-factor authentication	hss	modifyTwoFactorTopic
Ignoring web shells	hss	ignoreWebShell
Unignoring web shells	hss	notIgnoreWebShell

Operation	Resource Type	Trace Name
Uninstalling the agent	hss	unInstall
Setting a protection mode in WTP	hss	setProtectMode
Adding a protected file system in WTP	hss	addFileSystem
Removing a protected file system from WTP	hss	delFileSystem
Modifying a protected file system in WTP	hss	modifyFileSystem
Suspending protection for a file system in WTP	hss	suspendFileSystem
Resuming protection for a file system in WTP	hss	resumeFileSystem
Enabling unprotected periods in WTP	hss	turnonTimedStopProtect
Disabling unprotected periods in WTP	hss	turnoffTimedStopProtect
Setting unprotected periods in WTP	hss	setTimedStopDate
Adding unprotected periods in WTP	hss	addTimerRange
Modifying unprotected periods in WTP	hss	modifyTimerRange
Deleting unprotected periods from WTP	hss	delTimerRange
Setting WTP alarms	hss	setWtpAlertConfig
Enabling dynamic WTP	hss	turnonRasp
Disabling dynamic WTP	hss	turnoffRasp
Automatically isolating and killing malicious programs	hss	turnOnMPAutomatic
Stop isolating and killing malicious programs	hss	turnOffMPAutomatic
Importing the alarm whitelist	hss	importAlarmWhitelist
Removing alarms from whitelist	hss	deleteAlarmWhitelist
Managing the login whitelist	hss	operateLoginWhitelist
Managing events	hss	operateEventStatus

Operation	Resource Type	Trace Name
Cancel file isolation	hss	deleteProcessIsolation-Rule
Modifying a policy group	hss	modifyPolicyGroup
Removing a policy group	hss	deletePolicyGroup
Copying a policy group	hss	copyPolicyGroup
Modifying a policy group	hss	modifyPolicyContent
Applying a policy	hss	deployPolicyGroup
Adding a server group	hss	addHostGroup
Deleting a server group	hss	deleteHostGroup
Modifying a server group	hss	modifyHostGroup
Adding a server to a group	hss	insertHostGroup
Enabling or disabling file integrity management	hss	switchKeyfiles
Manage application recognition events	hss	operateAppWhiteListE-vent
Creating a whitelist policy	hss	replaceAppWhiteListPoli-cy
Enabling or disabling a whitelist policy	hss	switchAppWhiteListPolicy
Deleting a whitelist policy	hss	deleteAppWhiteListPolicy
Managing whitelisted applications	hss	operateAppWhiteListPo-licyApp
Removing a server associated with a policy	hss	deleteAppWhiteListHos-tInfo
Associating servers	hss	addAppWhiteListHostIn-fo
Managing ransomware events	hss	operateAppRansomEven-tInfo
Creating or editing a ransomware prevention policy	hss	replaceAppRansomPoli-cyInfo
Deleting a ransomware prevention policy	hss	deleteAppRansomPoli-cyInfo
Marking the ransomware status of a process	hss	operateAppRansomHa-shInfo

Operation	Resource Type	Trace Name
Removing a server associated with a ransomware prevention policy	hss	deleteAppRansomHos-tInfo
Associating a server with a ransomware prevention policy	hss	addAppRansomHostInfo
Relearning a ransomware prevention policy on associated servers	hss	relearnAppRansomHos-tInfo

12.2 Viewing Audit Logs

After you enable CTS, the system starts recording operations on HSS. Operation records for the last seven days can be viewed on the CTS console.

Viewing an HSS Trace on the CTS Console

Step 1 Log in to the management console.

Step 2 Click on the top of the page and choose **Cloud Trace Service** under **Management & Deployment**. The CTS console is displayed.

Step 3 Choose **Trace List** in the navigation pane.

Step 4 Click **Filter** and specify filtering criteria as needed. The following four filters are available:

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**.

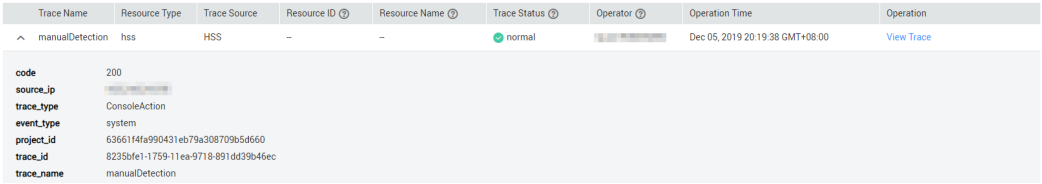
  Select the filter from the drop-down list.

  - Set **Trace Type** to **Management**.
  - Set **Trace Source** to **HSS**.
  - When you select **Trace name** for **Search By**, you also need to select a specific trace name. When you select **Resource ID** for **Search By**, you also need to select or enter a specific resource ID. When you select **Resource name** for **Search By**, you also need to select or enter a specific resource name.
- **Operator**: Select a specific operator (a user other than tenant).
- **Trace Rating**: Available options include **All trace status**, **normal**, **warning**, and **incident**. You can only select one of them.
- **Time Range**: In the upper right corner of the page, you can query traces in the last 1 hour, last 1 day, last 1 week, or within a customized period.

Step 5 Click **Query**.

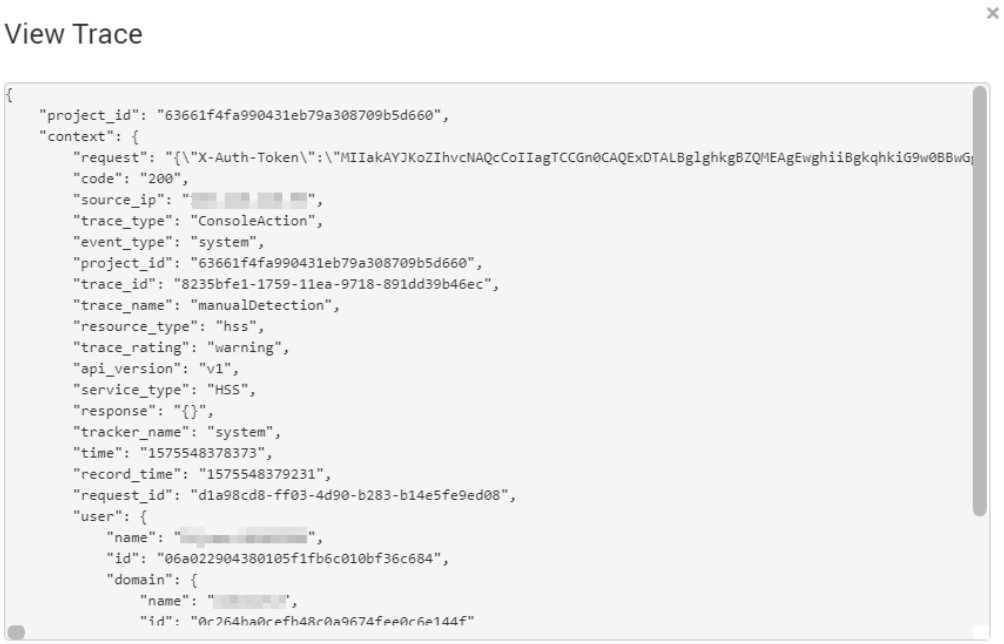
Step 6 Click on the left of a trace to expand its details, as shown in **Figure 12-1**.

Figure 12-1 Expanding trace details



Step 7 Click **View Trace** in the **Operation** column. On the displayed **View Trace** dialog box shown in **Figure 12-2**, the trace structure details are displayed.

Figure 12-2 Viewing a trace



----End

13 Permissions Management

13.1 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 **Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

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 permissions 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 policy

  A custom policy can contain the actions of multiple services that are of the project-level type. The following is an example policy containing actions of multiple services:

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

13.2 Actions

This section describes fine-grained permissions management for your HSS instances. If your 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 permissions policies to these groups. Users inherit permissions from the groups to which they are added and 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. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

Supported Actions

DNS 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. Actions supported by policies are specific to APIs. Common concepts related to policies include:

- Permission: A statement in a policy that allows or denies certain operations.
- Action: Specific operations that are allowed or denied.

- Dependent actions: When assigning an action to users, you also need to assign dependent permissions for that action to take effect.

A range of HSS actions can be defined in custom policies.

Actions

Permission	Action	Dependent Permission
Query the protected server list	hss:hosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list
Enable or disable protection on servers	hss:hosts:switchVersion	-
Manual scan	hss:hosts:manualDetect	-
Check the status of a manual scan	hss:manualDetectStatus:get	-
Query weak password scan reports	hss:weakPwds:list	-
Query account cracking protection reports	hss:accountCracks:list	-
Unblock an IP address that was blocked during account cracking prevention	hss:accountCracks:unblock	-
Query malicious program scan results	hss:maliciousPrograms:list	-
Query remote login scan results	hss:abnorLogins:list	-
Query important file change reports	hss:keyfiles:list	-
Query the open port list	hss:ports:list	-
Query the vulnerability list	hss:vuls:list	-
Perform batch operations on vulnerabilities	hss:vuls:operate	-
Query the account list	hss:accounts:list	-
Query the software list	hss:softwares:list	-

Permission	Action	Dependent Permission
Query the web path list	hss:webdirs:list	-
Query the process list	hss:processes:list	-
Query configuration scan reports	hss:configDetects:list	-
Query web shell scan results	hss:webshells:list	-
Query risky account scan reports	hss:riskyAccounts:list	-
Obtain server risk statistics	hss:riskyDashboard:get	-
Query password complexity policy scan reports	hss:complexityPolicys:list	-
Perform batch operations on malicious programs	hss:maliciousPrograms:operate	-
Perform batch operations on open ports	hss:ports:operate	-
Perform operations on detected unsafe settings	hss:configDetects:operate	-
Perform batch operations on web shells	hss:webshells:operate	-
Set common login locations	hss:commonLocations:set	-
Query common login locations	hss:commonLocations:list	-
Set common login IP addresses	hss:commonIPs:set	-
Query common login IP addresses	hss:commonIPs:list	-
Set the login IP address whitelist	hss:whiteIps:set	-
Query the login IP address whitelist	hss:whiteIps:list	-
Set weak passwords	hss:weakPwds:set	-

Permission	Action	Dependent Permission
Query weak passwords	hss:weakPwds:get	-
Set web paths	hss:webDirs:set	-
Query web paths	hss:webDirs:get	-
Obtain the list of servers where 2FA is enabled	hss:twofactorAuth:list	-
Set 2FA	hss:twofactorAuth:set	-
Enable or disable automatic isolation and killing of malicious programs	hss:automaticKillMp:set	-
Query the programs that have been automatically isolated and killed	hss:automaticKillMp:get	-
Query the agent download address	hss:installAgent:get	-
Uninstall the agent	hss:agent:uninstall	-
Query HSS alarms	hss:alertConfig:get	-
Set HSS alarms	hss:alertConfig:set	-
Query the WTP list	hss:wtpHosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list
Enable or disable WTP	hss:wtpProtect:switch	-
Set backup servers	hss:wtpBackup:set	-
Query backup servers	hss:wtpBackup:get	-
Set protected directories	hss:wtpDirectorys:set	-
Query the protected directory list	hss:wtpDirectorys:list	-
Query WTP records	hss:wtpReports:list	-
Set privileged processes	hss:wtpPrivilegedProcess:set	-
Query the privileged process list	hss:wtpPrivilegedProcess-es:list	-

Permission	Action	Dependent Permission
Set a protection mode	hss:wtpProtectMode:set	-
Query the protection mode	hss:wtpProtectMode:get	-
Set a protected file system	hss:wtpFilesystems:set	-
Query the protected file system list	hss:wtpFilesystems:list	-
Set scheduled protection	hss:wtpScheduledProtections:set	-
Query scheduled protection	hss:wtpScheduledProtections:get	-
Setting WTP alarms	hss:wtpAlertConfig:set	-
Query WTP alarms	hss:wtpAlertConfig:get	-
Query WTP statistics	hss:wtpDashboard:get	-
Query policy group	hss:policy:get	-
Set policy group	hss:policy:set	-
Query Application Recognition Service (ARS)	hss:ars:get	-
Set ARS	hss:ars:set	-
Query the detected intrusion list	hss:event:get	-
Perform operations on intrusions	hss:event:set	-
Query server groups	hss:hostGroup:get	-
Set server groups	hss:hostGroup:set	-
Monitor file integrity	hss:keyfiles:set	-
Query important file change reports	hss:keyfiles:list	-
Query the auto-startup list	hss:launch:list	-

14 FAQs

14.1 About HSS

14.1.1 What Is Host Security Service?

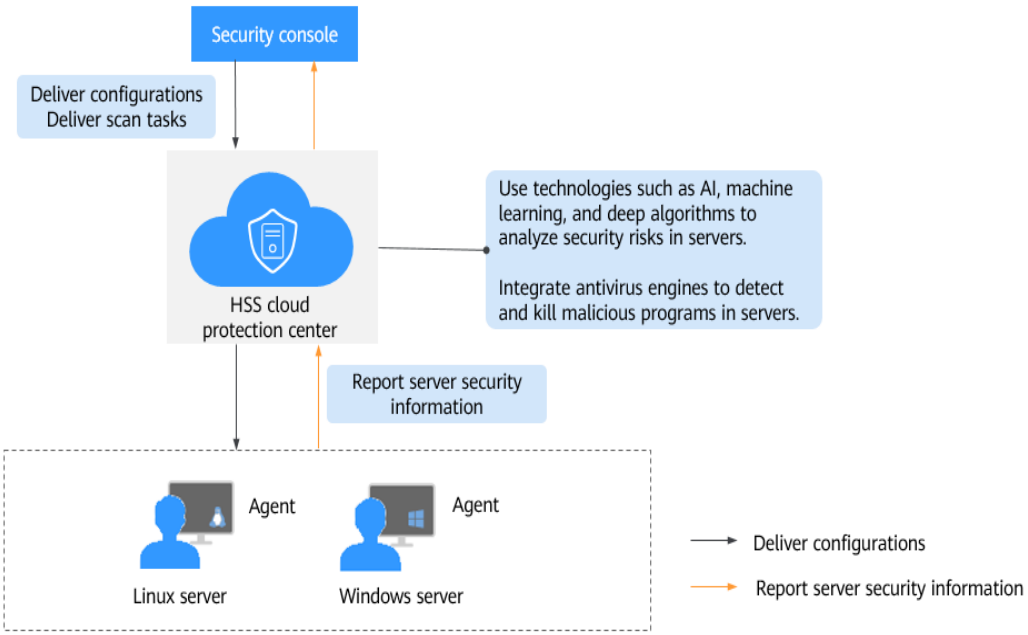
Host Security Service (HSS) helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

Working Principles

Install the HSS agent on your servers, and you will be able to check the server security status and risks in a region on the HSS console.

Figure 14-1 illustrates how HSS works.

Figure 14-1 Working principles



The following table describes HSS components.

Table 14-1 Components

Component	Description
Management console	A visualized management platform, where you can apply configurations in a centralized manner and view the defense status and scan results of servers in a region.
HSS cloud protection center	• Uses technologies such as AI, machine learning, and deep algorithms to analyze security risks in servers. • Integrates multiple antivirus engines to detect and kill malicious programs in servers. • Receives configurations and scan tasks sent from the console and forwards them to agents on the servers. • Receives server information reported by agents, analyzes security risks and exceptions on servers, and displays the analysis results on the console.

Component	Description
Agent	• Communicates with the HSS cloud protection center via HTTPS and WSS. Port 443 is used by default. • Scans all servers every early morning; monitors the security status of servers; and reports the collected server information (including non-compliant configurations, insecure configurations, intrusion traces, software list, port list, and process list) to the cloud protection center. • Blocks server attacks based on the security policies you configured. **NOTE** • If the agent is not installed or is abnormal, HSS is unavailable. • Select the agent and installation command suitable for your OS. • Web Tamper Protection (WTP) and HSS can use the same agent on a server.

14.1.2 What Is the HSS Agent?

The HSS agent is used to perform scans on all servers, monitor server security status in real time, and reports collected server information to the cloud protection center.

Functions of the Agent

- The agent runs scan tasks every day in the early morning to scan all servers, monitors server security, and reports collected server information to the cloud protection center.
- The agent blocks server attacks based on the security policies you configured.

NOTE

- If the agent is not installed or is abnormal, HSS is unavailable.
- WTP and HSS can use the same agent on a server.

Linux Agent Processes

The agent process needs to be run by the **root** user.

The agent contains the following processes:

Table 14-2 Linux agent processes

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

Agent Process Name	Function	Path
upgrade	Upgrades the agent.	/usr/local/hostguard/bin/upgrade

Windows Agent Processes

The agent process needs to be run by the **system** user.

The agent contains the following processes:

Table 14-3 Windows agent processes

Agent Process Name	Function	Path
HostGuard.exe	Detects and protects the system against security issues.	C:\Program Files (x86)\HostGuard\HostGuard.exe
HostWatch.exe	Monitors the agent process.	C:\Program Files (x86)\HostGuard\HostWatch.exe
upgrade.exe	Upgrades the agent.	C:\Program Files (x86)\HostGuard\upgrade.exe

14.2 Deployment and Configuration

14.2.1 Is the Agent in Conflict with Any Other Security Software?

Yes, it may be in conflict with DenyHosts.

- Symptom: The IP address of the login host is identified as an attack IP address but cannot be unblocked.
- Cause: HSS and DenyHosts both block possible attack IP addresses, but HSS cannot unblock the IP addresses that were blocked by DenyHosts.
- Handling method: Stop DenyHosts.

1. Log in as user **root** to ECS.
2. Run the following command to check whether DenyHosts has been installed:

   ps -ef | grep denyhosts.py

   If information similar to the following is displayed, DenyHosts has been installed:

```
[root@hss-test ~]# ps -ef | grep denyhosts.py
root      64498      1  0 17:48 ?        00:00:00 python denyhosts.py --daemon
```

3. Run the following command to stop DenyHosts:

   kill -9 'cat /var/lock/denyhosts'

4. Run the following command to cancel the automatic start of DenyHosts upon host startup:

   chkconfig --del denyhosts;

14.2.2 How Do I Install the Agent?

- For details about how to install the Linux agent, see **Installing an Agent on the Linux OS**.
- For details about how to install the Windows agent, see **Installing an Agent on the Windows OS**.

14.2.3 What Is the Default Agent Installation Path?

The agent installation paths on servers running the Linux or Windows OS cannot be customized. **Table 14-4** describes the default paths.

Table 14-4 Default agent installation paths

OS	Default Installation Path
Linux	/usr/local/hostguard/
Windows	C:\Program Files (x86)\HostGuard

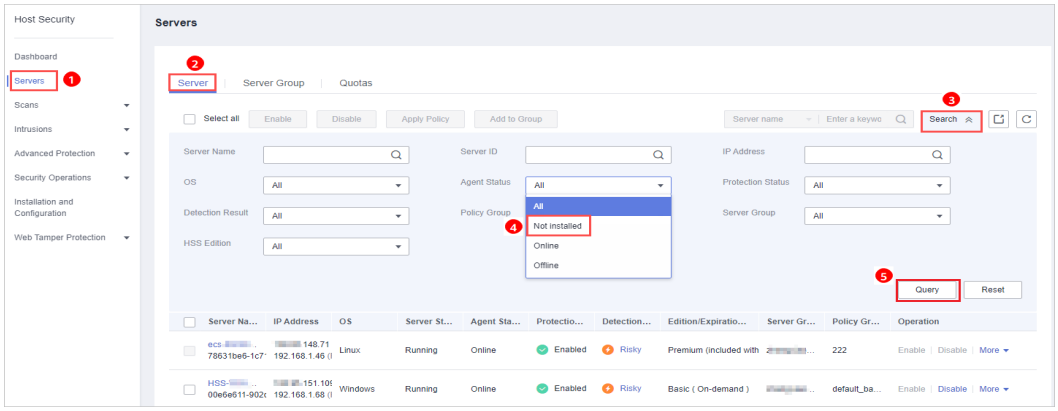
14.2.4 How Do I Filter Servers Where No Agents Have Been Installed?

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** > **Host Security Service**.

Step 3 On the **Servers** page, filter the servers where no agents have been installed, as shown in **Figure 14-2**.

Figure 14-2 Filtering the servers where no agents have been installed



Possible agent statuses are:

- **Not installed**: The agent has not been installed or successfully started.
- **Online**: The agent is running properly.
- **Offline**: The communication between the agent and the HSS server is abnormal, and HSS cannot protect your servers.

  You can click **Offline**, and view servers whose agents are offline and the offline reasons at the bottom of the page that is displayed.

----End

14.2.5 What Should I Do If the Agent Status Is Abnormal?

If the agent status is **Not installed** or **Offline**, the communication between the agent and the server is abnormal. Main statuses are as follows:

- **Uninstalled**: No agent has been installed on the server, or the agent has been installed but not started.
- **Offline**: The communication between the agent and the server is abnormal. The agent on the server has been deleted, or a server is offline.
- **Online**: The agent on the server is running properly.

Possible Causes

- The network is faulty.

  The agent or the cloud protection center is abnormal. For example, the NIC is faulty, the IP address changes, or the bandwidth is low.
- The agent process is abnormal.
- The agent status has not been updated. After the agent is installed, it takes about 2 minutes for the console to update its status.

Solution

Step 1 Fix network problems (if any).

After the network recovers,

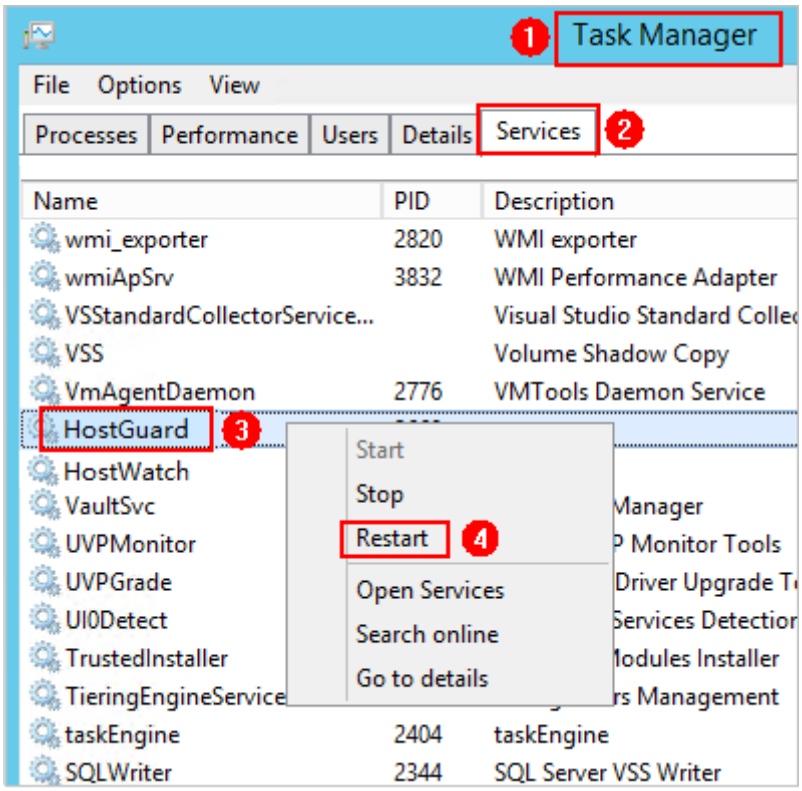
- If the agent status is **Online**, no further action is required.
- If the agent status is **Not installed** or **Offline**, go to **Step 2**.

Step 2 Log in to the server and restart the agent. The agent status **Not installed** or **Offline** indicates that the agent process is probably abnormal.

- Windows OS

  Log in to the server as **administrator** and restart the client.

Figure 14-3 Restarting Windows agent



- Linux OS

  Run the following command in the CLI as user **root** to restart the agent:

  service hostguard restart

  If the following information is displayed, the restart is successful:

  ```
  root@HSS-Ubuntu32:~#service hostguard restart
  Stopping Hostguard...
  Hostguard stopped
  Hostguard restarting...
  Hostguard is running
  ```

After the process is restarted, wait for about 2 minutes.

- If the agent status is **Online**, no further action is required.
- If the agent status is still **Not installed** or **Offline**, uninstall the agent and install it again.

----End

14.2.6 How Do I Uninstall the Agent?

Scenario

- The agent was installed using an incorrect package and you need to uninstall it.
- The agent was installed using incorrect commands and you need to uninstall it.

Prerequisites

- Login credentials have been obtained.
- **Agent Status** of the server is **Online**.

Uninstalling the Agent on the Console in One Click

You can uninstall an HSS agent from the HSS console.

NOTE

After the agent is uninstalled from a server, HSS will not provide any protection for the server.

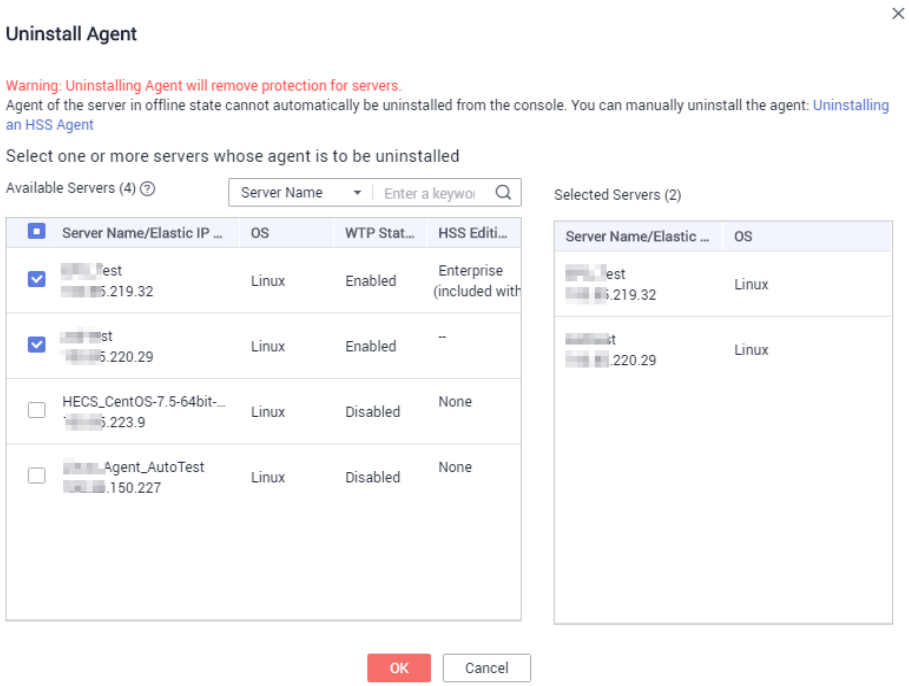
Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Security Operations** > **Installation and Configuration**. In the upper right corner of the **Installation and Configuration** page, click **Uninstall Agent**.

Step 4 On the **Uninstall Agent** page, select the server whose agent is to be uninstalled.

Figure 14-4 Uninstalling an agent



Step 5 Click **OK**.

In the server list, if **Agent Status** of the server is **Offline**, its agent is successfully uninstalled.

----End

Uninstalling the Agent from the Server

You can manually uninstall an HSS agent on a server when you no longer use HSS or need to reinstall the agent.

NOTE

After the agent is uninstalled from a server, HSS will not provide any protection for the server.

- **Uninstalling the Linux agent**
  a. Log in to the server from which you want to uninstall the agent. Then run the **su - root** command to switch to user **root**.
  b. In any directory, run the following command to uninstall the agent:
     i. If the agent was installed using an .rpm package, run the **rpm -e --nodeps hostguard** command.
     ii. If the agent was installed using a .deb package, run the **dpkg -P hostguard** command.

     If the following information is displayed, the agent is uninstalled:

     ```
     Stopping Hostguard...
     Hostguard stopped
     Hostguard uninstalled.
     ```

- **Uninstalling the Windows agent**
  a. Log in to the server from which you want to uninstall an HSS agent.
  b. Click **Start** and choose **Control Panel** > **Programs**. Then select **HostGuard** and click **Uninstall**.

     NOTE

     - Alternatively, go to the installation directory and double-click **unins000.exe**.
     - 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.

  c. In the **Uninstall HostGuard** dialog box, click **Yes**.
  d. After the uninstallation is complete, click **OK**.

14.3 Alarm and Event Management

14.3.1 Brute-force Attack Defense

14.3.1.1 How Do I Block Brute-Force Attacks?

Protection Scope

HSS can block attacks on MySQL, MS SQL, VSFTP, FileZilla, Serv-U, SSH, and RDP.

If MySQL or VSFTP is installed on your server, after HSS is enabled, the agent will add rules to iptables to prevent MySQL and VSFTP brute force attacks. When detecting a brute-force attack, HSS will add the source IP address to the blocking list. The added rules are highlighted below.

Figure 14-5 Added rules

NOTICE

Existing iptables rules are used for blocking brute-force attacks. You are advised to keep them. If they are deleted, HSS will not be able to protect MySQL or VSFTP from brute-force attacks.

How Brute-Force Attacks Are Blocked

Brute-force attacks are a type of common intrusion attacks. Attackers submit many server passwords until eventually guessing correctly and gaining control over a server.

HSS uses brute-force detection algorithms and an IP address blacklist to effectively prevent brute-force attacks and block attacking IP addresses. The blocking duration for suspicious SSH attacks is 12 hours and that for other suspicious attacks is 24 hours. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked. HSS supports 2FA to authenticate user identity, effectively blocking account attacks.

NOTE

If HSS detects account cracking attacks on servers using Kunpeng EulerOS (EulerOS with ARM), it does not block the source IP addresses and only generates alarms. The SSH login IP address whitelist does not take effect for such servers.

Alarm Policies

- If a hacker successfully cracks the password and logs in to a server, a real-time alarm will be immediately sent to specified recipients.
- If a brute-force attack and risks of account hacking are detected, a real-time alarm will be immediately sent to specified recipients.
- If a brute-force attack is detected and failed, and no unsafe settings (such as weak passwords) are detected on the server, no real-time alarms will be sent. HSS will summarize all attacks in a day in its daily alarm report. You can also view block attacks on the **Intrusions** page of the HSS console.

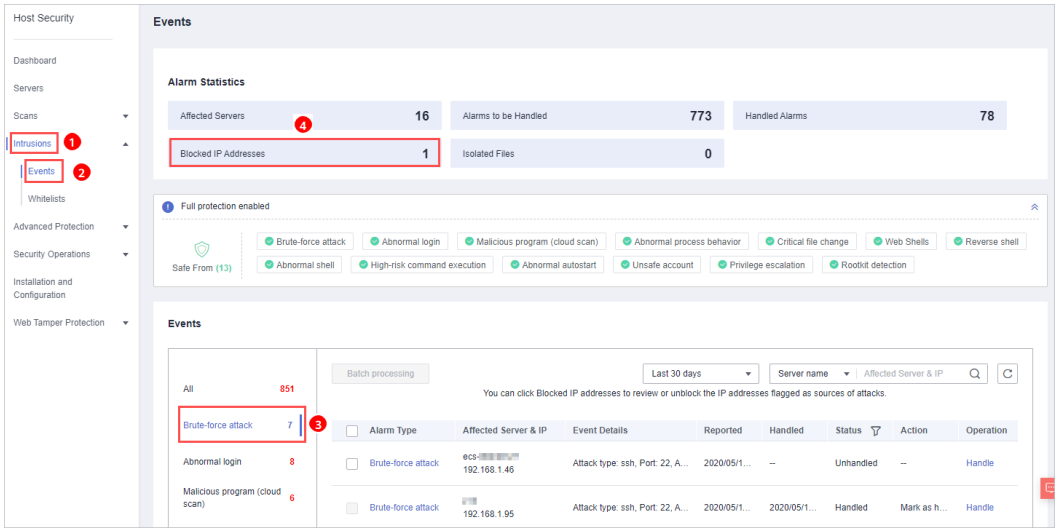
Viewing Account Cracking Detection Results

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** > **Host Security Service**.

Step 3 In the table displayed after you click **Brute-force attack**, you can view blocked attacks on protected servers.

Figure 14-6 Brute-force attack



Step 4 Click **Blocked IP Addresses** to check the source IP addresses, attack types, number of intercepted attacks, the time of the first and last interceptions, and the interception status.

- **Blocked** indicates the brute-force attack has been blocked by HSS.
- **Canceled** indicates you have unblocked the source IP address of the brute force attack.

  NOTE

  By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours. If a blocked IP address does not perform brute-force attacks in the default blocking duration, it will be automatically unblocked.

----End

Managing Blocked IP Addresses

- If a server is frequently attacked, you are advised to fix its vulnerabilities in a timely manner and eliminate risks.
- If a valid IP address is blocked by mistake (for example, after O&M personnel enter incorrect passwords for multiple times), manually unblock the IP address.

NOTICE

After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address.

14.3.1.2 What Should I Do If the Account Cracking Prevention Function Does Not Take Effect on Some Accounts in Linux OSs?

Possible Causes

The SSHD service in the host system does not depend on **libwrap.so**.

NOTE

As a free software library, libwrap implements the universal TCP Wrapper function. Any daemon that contains **libwrap.so** can use the rules in files **/etc/hosts.allow** and **/etc/hosts.deny** to perform simple access control on the host.

Solution

Log in to the server and install the HSS agent. Then run the following command:

sh /usr/local/hostguard/conf/config_ssh_xinetd.sh.

Affected Image Versions

- The following are SUSE images that have the problem:
  - SUSE Enterprise 12 SP2 64bit (40 GB)
  - SUSE Enterprise 12 SP2 64bit for SAP (100 GB)
  - SAP HANA express edition Server only
  - SAP HANA express edition XS Advanced Application
- The following are Gentoo images that have the problem:
  - Gentoo Linux 17.0 64bit (40 GB)
  - Gentoo Linux 13.0 64bit (40 GB)
- The following are OpenSUSE images that have the problem:
  - OpenSUSE 42.2 64bit (40 GB)
  - OpenSUSE 13.2 64bit (40 GB)

14.3.2 Weak Passwords and Unsafe Accounts

14.3.2.1 How Do I Handle a Weak Password Alarm?

Servers using weak passwords are exposed to intrusions. If a weak password alarm is reported, you are advised to change the alarmed password immediately.

Causes

- If simple passwords are used and match those in the weak password library, a weak password alarm will be generated.
- A password used by multiple member accounts will be regarded as a weak password and trigger an alarm.

Checking and Changing Weak Passwords

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** > **Host Security Service**.

Step 3 Choose **Scans** > **Unsafe Settings** and click the **Common Weak Password Detection** tab.

Step 4 Check the server, account name, account type, and usage duration of the alarmed weak password. Log in to the server and change the password.

----End

Changing a Weak Password

System	Procedure	Remarks
Windows OS	To change the password in the Windows 10, perform the following steps: 1. Log in to the Windows OS. 2. Click  in the lower left corner and click  . 3. In the **Windows Settings** window, click **Accounts**. 4. Choose **Sign-in options** from the navigation tree. 5. On the **Sign-in options** tab, click **Change** under **Password**.	None
Linux OS	Log in to the Linux server and run the following command: **passswd [*<user>*]**	Replace *<user>* with the username. If you do not specify any username, you are changing the password of the current user. After the command is executed, enter the new password as prompted.

System	Procedure	Remarks
MySQL database	1. Log in to the MySQL database. 2. Run the following command to check the database user password: **SELECT user, host, authentication_string From user;** This command is probably invalid in certain MySQL versions. In this case, run the following command: **SELECT user, host password From user;** 3. Run the following command to change the password: **SET PASSWORD FOR'*Username*'@'*Host*'=PASSWORD('*New_password*');** 4. Run the following command to refresh password settings: **flush privileges;**	None
Redis database	1. Open the Redis database configuration file **redis.conf**. 2. Run the following command to change the password: **requirepass *<password>*;**	Replace *<password>* with the new password. If there is already a password, the command will change it to the new password. If there has been no password set, the command will set the password.
Tomcat	1. Open the **conf/tomcat-user.xml** configuration file in the Tomcat root directory. 2. Change the value of **password** under the **user** node to a strong password.	None

14.3.2.2 How Do I Set a Secure Password?

Comply with the following rules:

- Use a password with high complexity.

  The password must meet the following requirements:

a. Contains at least eight characters.
b. Contain at least three types of the following characters:
   i. Uppercase letters (A-Z)
   ii. Lowercase letters (a-z)
   iii. Digital (0-9)
   iv. Special characters: space and `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
c. The password cannot be the username or the username in reverse order.

   Bad password examples: **administrator**, **test**, **root**, **oracle**, **mysql**

- Do not use common weak passwords that are easy to crack, including:
  - Birthday, name, ID card, mobile number, email address, user ID, time, or date
  - Consecutive digits and letters, adjacent keyboard characters, or passwords in rainbow tables

    Bad examples: **123456**, **abcdef**, **123abc**, **qwerty**, **1qaz2wsx**, **!QAZxsw2**, **qazxsw**, **1qaz@WSX**, **1q2w3e**, **123456789**, **password**
  - Phrases

    Bad examples: **143**, **iloveyou**
  - Common words, such as company names, **admin**, and **root**
- Do not use empty or default passwords.
- Do not reuse the latest five passwords you used.
- Use different passwords for different websites and accounts.
- Do not use the same pair of username and password for multiple systems.
- Change your password at least once every 90 days.
- If an account has an initial password, force the user to change the password upon first login or within a limited period of time.
- You are advised to set a locking policy for all accounts. If the consecutive login failures of an account exceed five times, the account will be locked, and will be automatically unlocked in 30 minutes.
- You are advised to set a logout policy. Accounts that have been inactive for more than 10 minutes will be automatically logged out or locked.
- You are advised to force users to change the initial passwords of their accounts upon their first login.
- You are advised to retain account login logs for at least 180 days. The logs cannot contain user passwords.

14.3.3 Unsafe Settings

14.3.3.1 How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS?

Installing a PAM

Your password complexity policy cannot be checked if no pluggable authentication module (PAM) is running in your system.

For Debian or Ubuntu, run the **apt-get install libpam-cracklib** command as the administrator to install a PAM.

NOTE

A PAM is installed and running by default in CentOS, Fedora, and EulerOS.

Setting a Password Complexity Policy

A proper password complexity policy would be: eight characters for the length of a password and at least three types of the following characters used: uppercase letters, lowercase letters, digits, and special characters.

NOTE

The preceding configurations are basic security requirements. For more security configurations, run the following commands to obtain help information in Linux OSs:

- For CentOS, Fedora, and EulerOS based on Red Hat 7.0, run:
  man pam_pwquality
- For other Linux OSs, run:
  man pam_cracklib

- CentOS, Fedora, and EulerOS
  a. Run the following command to edit the **/etc/pam.d/system-auth** file:
     vi /etc/pam.d/system-auth
  b. Find the following information in the file:
     - For CentOS, Fedora, and EulerOS based on Red Hat 7.0:
       password requisite pam_pwquality.so try_first_pass retry=3 type=
     - For other CentOS, Fedora, and EulerOS systems:
       password requisite pam_cracklib.so try_first_pass retry=3 type=
  c. Add the following parameters and their values: **minlen**, **dcredit**, **ucredit**, **lcredit**, and **ocredit**. If the file already has these parameters, change their values. For details, see **Table 14-5**.
     Example:
     password requisite pam_cracklib.so try_first_pass retry=3 minlen=9 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 type=

     NOTE

     At least three of **dcredit**, **ucredit**, **lcredit**, and **ocredit** must be set to negative numbers.

Table 14-5 Parameter description

Parameter	Description	Example
minlen	Minimum length of a password. A PAM uses **credits** by default. As a result, the minimum password length is one plus. For example, if you want the minimum length to be eight, set the **minlen** value to **9**.	minlen=9
dcredit	Number of digits A negative value (for example, **-N**) indicates the number (for example, N) of digits required in a password. A positive value indicates that there is no limit.	dcredit=-1
ucredit	Number of uppercase letters A negative value (for example, **-N**) indicates the number (for example, N) of uppercase letters required in a password. A positive value indicates that there is no limit.	ucredit=-1
lcredit	Number of lowercase letters A negative value (for example, **-N**) indicates the number (for example, N) of lowercase letters required in a password. A positive value indicates that there is no limit.	lcredit=-1
ocredit	Number of special characters A negative value (for example, **-N**) indicates the number (for example, N) of special characters required in a password. A positive value indicates that there is no limit.	ocredit=-1

- Debian and Ubuntu
  a. Run the following command to edit the **/etc/pam.d/common-password** file:

     vi /etc/pam.d/common-password

  b. Find the following information in the file:

     password requisite pam_cracklib.so retry=3 minlen=8 difok=3

  c. Add the following parameters and their values: **minlen**, **dcredit**, **ucredit**, **lcredit**, and **ocredit**. If the file already has these parameters, change their values. For details, see **Table 14-5**.

     Example:

password requisite pam_cracklib.so retry=3 minlen=9 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 difok=3

14.3.3.2 How Do I Set a Proper Password Complexity Policy in a Windows OS?

A proper password complexity policy would be: eight characters for the length of a password and at least three types of the following characters used: uppercase letters, lowercase letters, digits, and special characters.

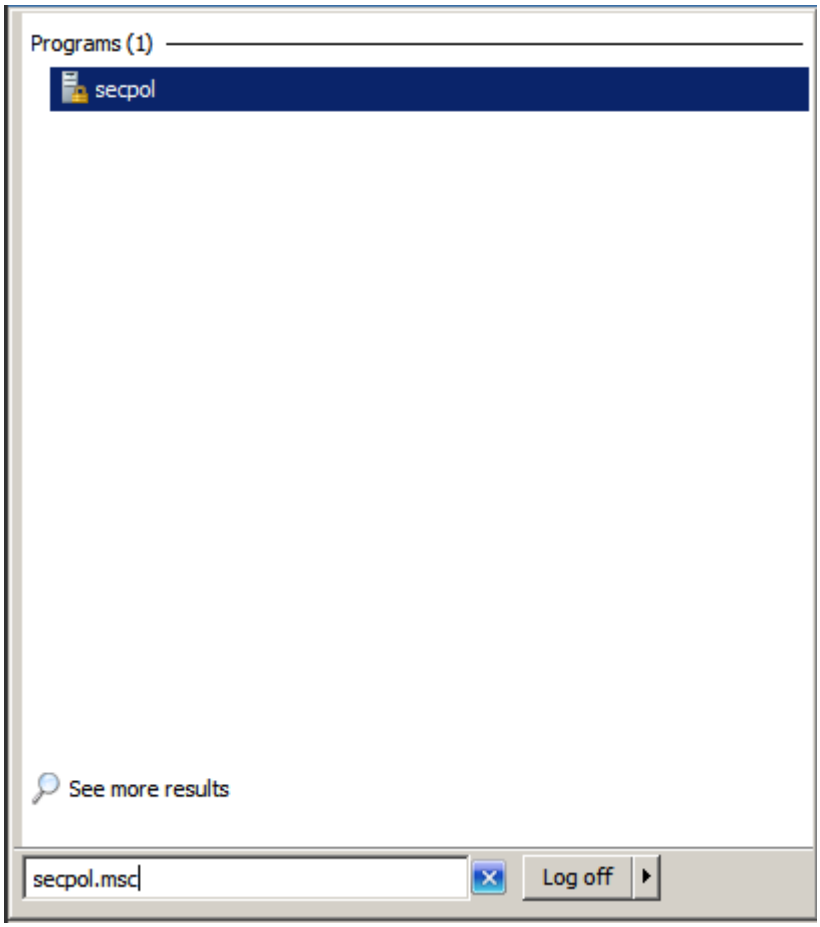
Perform the following steps to set a local security policy:

Step 1 Log in to the OS as user **Administrator**. Choose **Start** > **Control Panel** > **System and Security** > **Administrative Tools**. In the **Administrative Tools** folder, double-click **Local Security Policy**.

NOTE

Alternatively, click **Start** and type **secpol.msc** in the **Search programs and files** box, as shown in **Figure 14-7**.

Figure 14-7 Using the search box

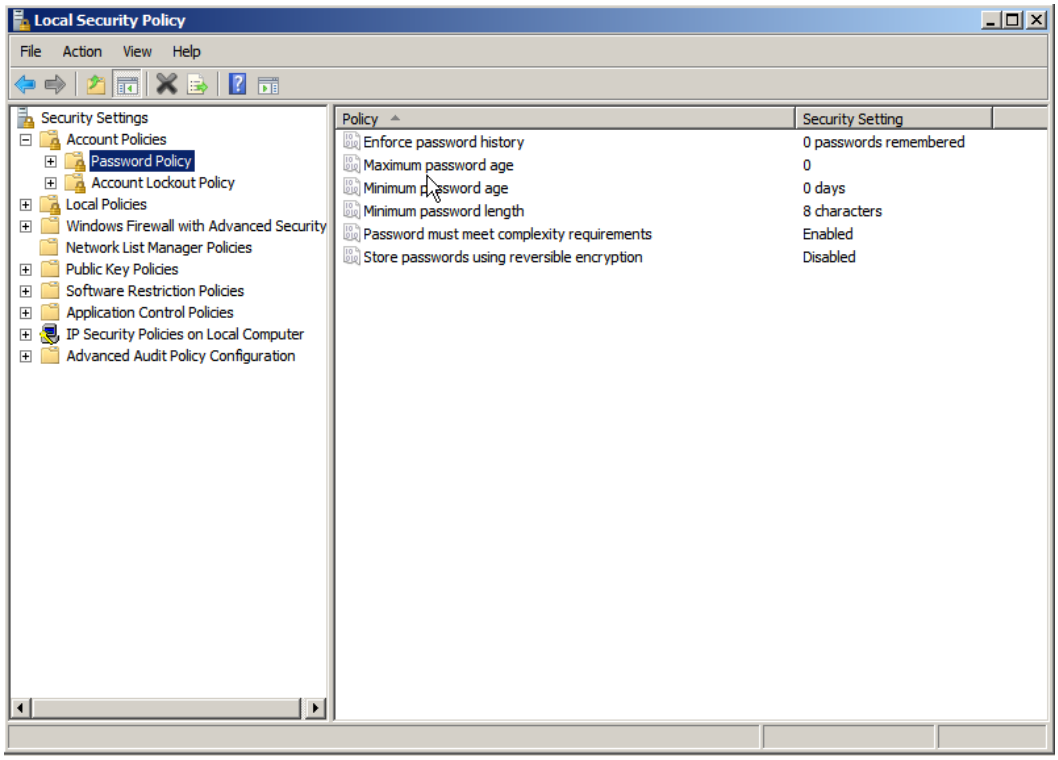


Step 2 Choose **Account Policies** > **Password Policy** and perform the following operations, as shown in **Figure 14-8**.

- Double-click **Password must meet complexity requirements**, select **Enable**, and click **OK** to enable the policy.

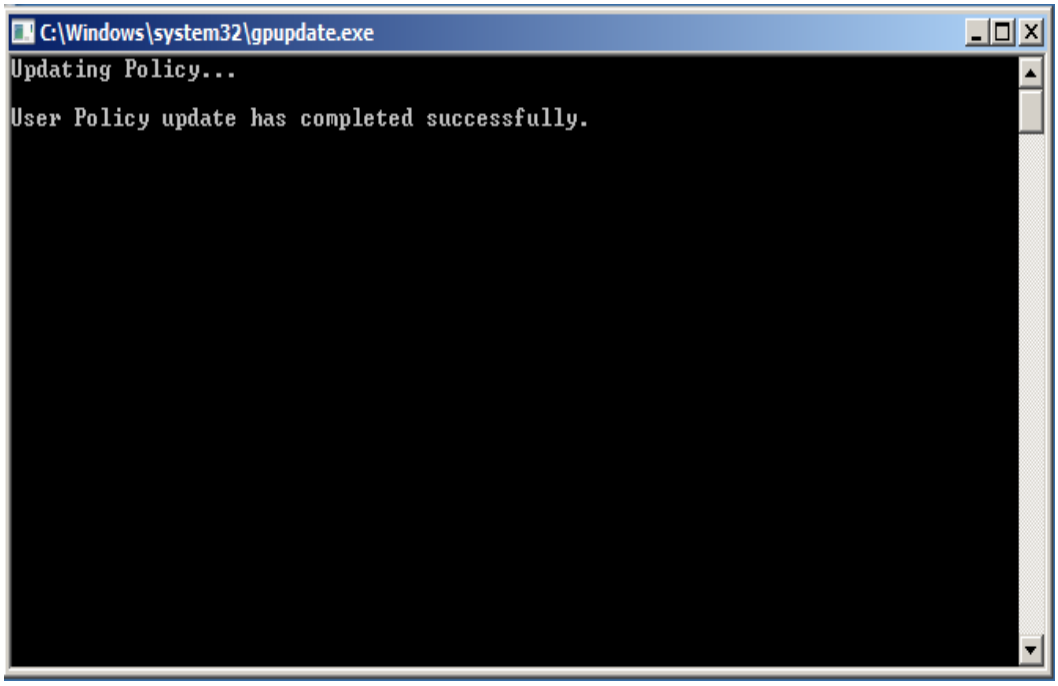
- Double-click **Minimum password length**, enter the length (greater than or equal to **8**), and click **OK** to set the policy.

Figure 14-8 Configuring local security policies



Step 3 Run the **gpupdate** command to refresh your system settings. **Figure 14-9** shows that the refresh is successful and the settings are applied in the system.

Figure 14-9 Execution result



----End

14.4 Vulnerability Management

14.4.1 How Do I Fix Vulnerabilities?

Procedure

Step 1 Check the vulnerability detection results.

Step 2 Based on provided solutions, fix vulnerabilities one by one in descending order by severity.

- Restart the Windows OS after you fix its vulnerabilities.
- Restart the Linux OS after you fix its kernel vulnerabilities.

Step 3 HSS scans all Linux, Windows, and Web-CMS servers for vulnerabilities every early morning. After you fix the vulnerabilities, you are advised to perform a check immediately to verify the result. For details, see **Starting a Software Vulnerability Detection**.

----End

14.4.2 What Should I Do If a Warning Still Exists After I Fixed a Vulnerability as Prompted?

Solution

- After the vulnerability is fixed, you are advised to check the software upgrade result to ensure that the software has been upgraded to the latest version.

- After the vulnerability is fixed, you are advised to perform a manual detection to verify the result. For details, see **Starting a Software Vulnerability Detection**.

NOTE

HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.

14.4.3 Why the Alarms of Fixed Vulnerabilities Are Still Displayed?

HSS performs a full check every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.

Perform the following steps to check the latest fix result:

Step 1 Check the software upgrade result to ensure that the software has been upgraded to the latest version. For details about the operation commands, see **Table 14-6**.

Table 14-6 Verification commands

OS	Verification Command
CentOS/Fedora /Euler/ Redhat/Oracle	rpm -qa | grep *Software_name*
Debian/Ubuntu	dpkg -l | grep *Software_name*
Gentoo	emerge --search *Software_name*
SUSE	zypper search -dC --match-words *Software_name*

Step 2 **Manually check for software vulnerabilities** and view the vulnerability fixing result.

----End

14.4.4 Why a Server Displayed in Vulnerability Information Does Not Exist?

Vulnerabilities detected in the past 24 hours are displayed. The server name in a vulnerability notification is the name used when the vulnerability was detected, and may be different from the latest server name.

14.4.5 Do I Need to Restart a Server After Fixing its Vulnerabilities?

- For a Windows server, you need to restart it after you fix its vulnerabilities.
- For a Linux server, you need to restart it if you have fixed its kernel vulnerabilities.

14.5 Web Tamper Protection

14.5.1 Why Do I Need to Add a Protected Directory?

WTP protects files in directories. If no directories are specified, WTP cannot take effect even if it is enabled.

14.5.2 How Do I Modify a Protected Directory?

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** > **Host Security Service**.

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

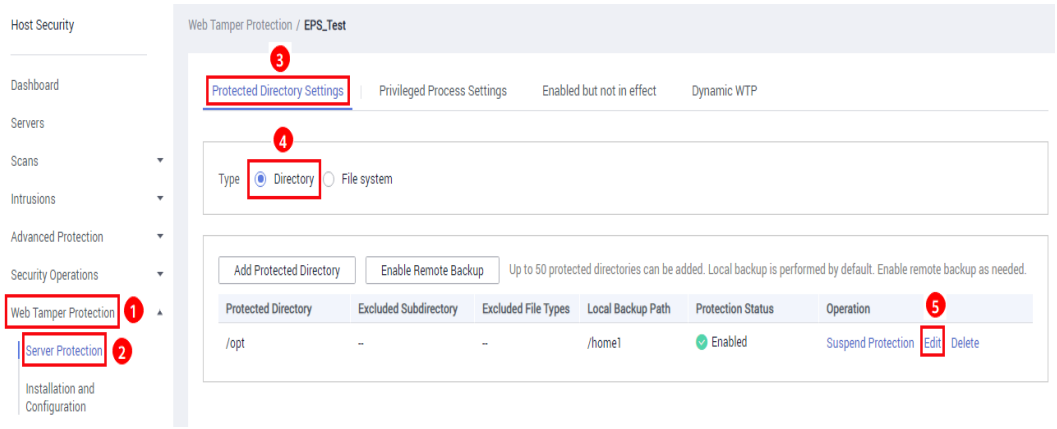
Step 4 Locate the target server and click **Configure Protection** in the **Operation** column.

Step 5 Select the required protected directory and click **Edit** in the **Operation** column.

NOTE

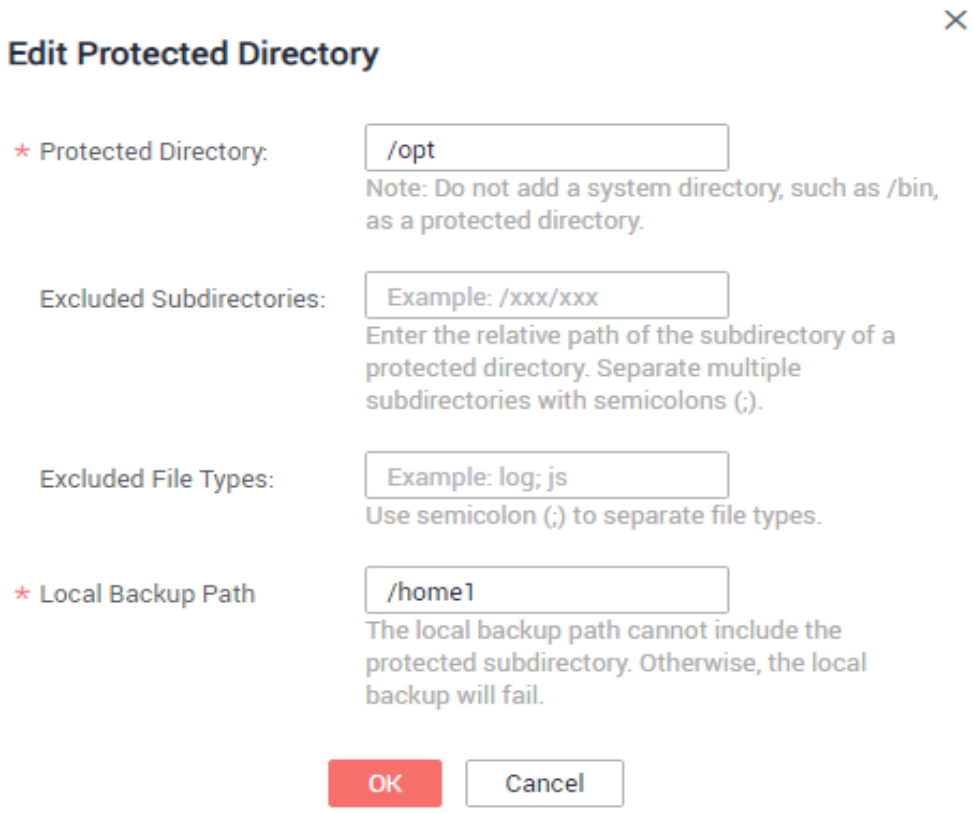
- If you need to modify files in the protected directory, stop protection for the protected directory first.
- After the files are modified, resume protection for the directory in a timely manner.

Figure 14-10 Configuring protection



Step 6 In the **Edit Protected Directory** dialog box, modify the settings and click **OK**.

Figure 14-11 Editing protected directory



----End

14.5.3 How Do I Modify a File After WTP Is Enabled?

Protected directories are read-only. To modify files or update the website, perform any of the following operations.

Specifying Privileged Processes

Privileged processes have the permission to modify files.

- Privileged processes can access protected directories. Ensure that privileged processes are secure and reliable.
- On Linux servers, privileged processes take effect only if **Type** is set to **File system** on the **Protected Directory Settings** tab.

Temporarily Disabling WTP

Disable WTP while you modify files in protected directories.

Your website is not protected from tampering while WTP is disabled. Enable it immediately after updating your website.

Setting Scheduled Protection

You can set periodic static WTP, and update websites while WTP is automatically disabled.

Exercise caution when you set the periods to disable WTP, because files will not be protected in those periods.

14.5.4 What Can I Do If I Enabled Dynamic WTP But Its Status Is Enabled but not in effect?

Dynamic WTP protects your Tomcat applications.

For this function to take effect, ensure that:

- There are Tomcat applications running on your servers.
- Your servers run the Linux OS.
- The **setenv.sh** file has been automatically generated in the **tomcat/bin** directory (usually 20 minutes after you enable dynamic WTP). If the file exists, restart Tomcat to make dynamic WTP take effect.

If the status of dynamic WTP is **Enabled but not in effect** after you enable it, perform the following operations:

- Check whether the **setenv.sh** file has been generated in the **tomcat/bin** directory.
- If the **setenv.sh** file exists, check whether Tomcat has been restarted.

14.6 Others

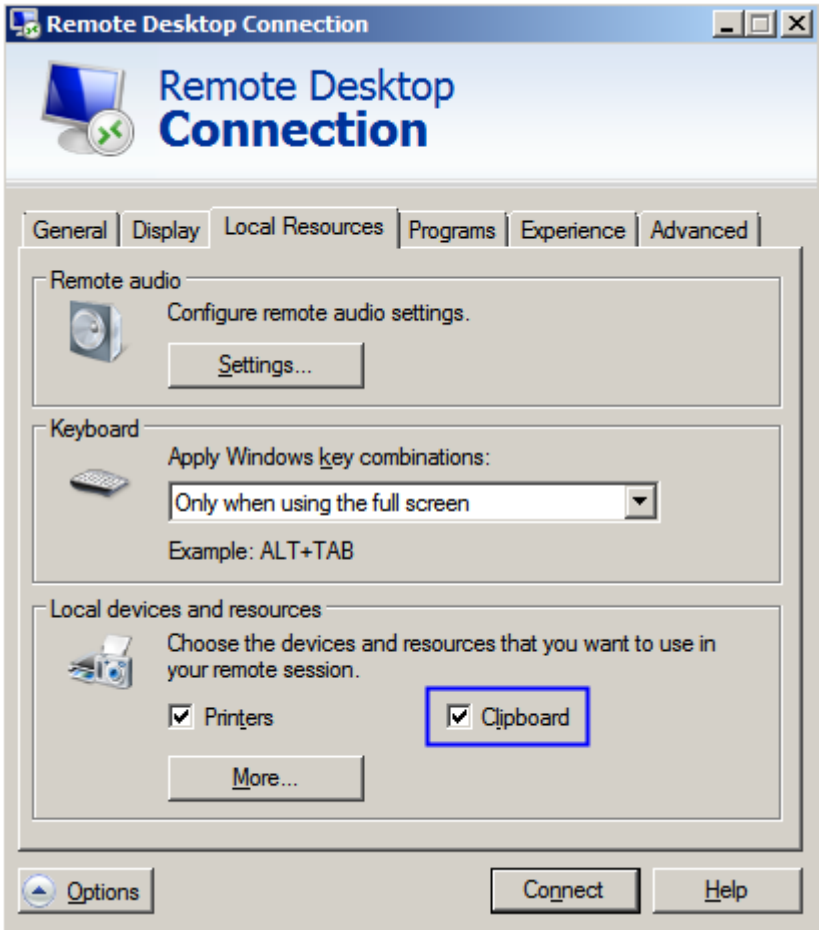
14.6.1 How Do I Use the Windows Remote Desktop Connection Tool to Connect to a Server?

Procedure

Step 1 On the local PC, choose **Startup** > **Running**, and then run the **mstsc** command to start Windows Remote Desktop Connection.

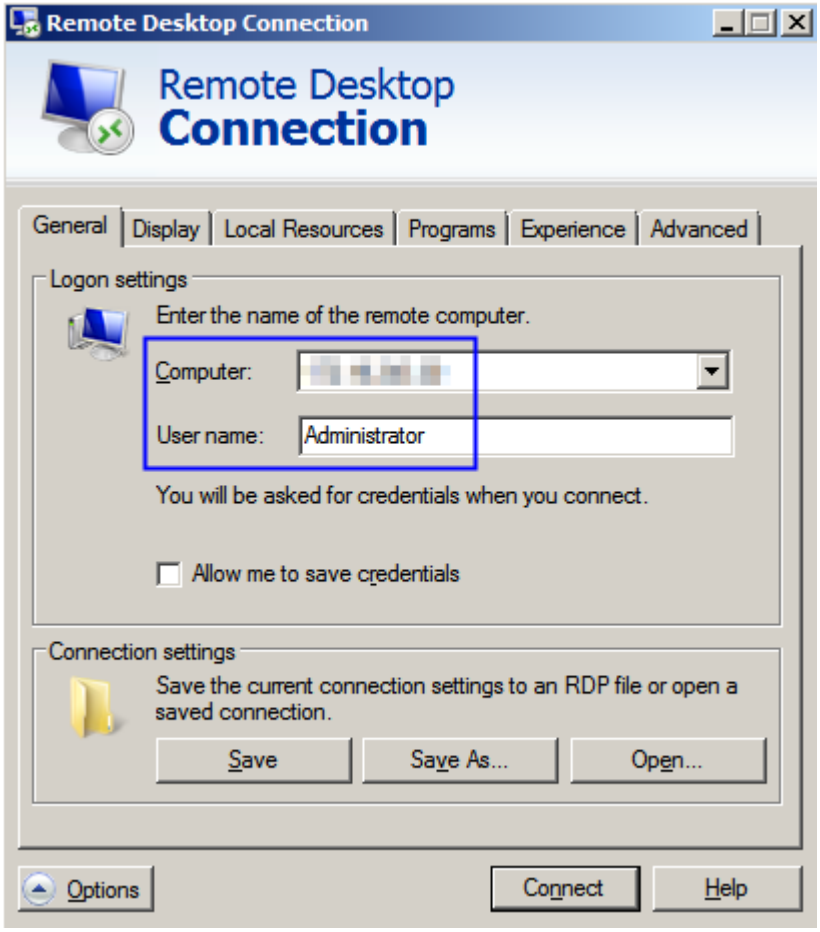
Step 2 Click **Options**, and then click the **Local Resources** tab. In the **Local devices and resources** area, select **Clipboard**.

Figure 14-12 Remote desktop connection



Step 3 Click the **General** tab. In **Computer**, enter the EIP of the server on which you want to install an agent. In **User name**, enter **Administrator**. Then click **Connect**.

Figure 14-13 Setting general parameters



Step 4 In the displayed dialog box, enter the user password of the server and click **OK** to connect to the server.

----End

14.6.2 How Do I Check HSS Log Files?

Log Paths

The following table describes log files and their paths.

OS	Log Directory	Log File
Linux	/usr/local/hostguard/log/	• **daemon.log**: daemon process runtime log • **hostguard.log**: monitoring process runtime log • **hostguard_procmon.log**: process creation log • **urlconfig.log**: region log. This is used only during installation.

OS	Log Directory	Log File
Windows	C:\Program Files (x86)\HostGuard\log\	• **daemon.log**: upgrade.log • **hostguard_rsync.log**: run log of the WTP backup server

Log Retention

Log File	Maximum Size	Retained File	Retention Period
daemon.log	10 MB	Latest five **daemon.log** files	Until the HSS agent is uninstalled
hostguard.log	10 MB	Latest five **hostguard.log** files	
hostguard_procmon.log	20 MB	Latest two **hostguard_procmon.log** files	
urlconfig.log	Unlimited	Only one **urlconfig.log** file	
upgrade.log	Unlimited	Only one **upgrade.log** file	
hostguard_rsync.log	Unlimited	Only one **hostguard_rsync.log** file	

14.6.3 How Do I Enable Logging for Login Failures?

MySQL

The account hacking prevention function for both Windows and Linux OSs supports MySQL 5.6 and 5.7. Perform the following steps to enable logging for login failure:

Step 1 Log in to the host as the **root** user.

Step 2 Run the following command to query the **log_warnings** value:

show global variables like 'log_warnings'

Step 3 Run the following command to change the **log_warnings** value:

set global log_warnings=2

Step 4 Modify the configuration file.

- For a Windows OS, modify the **my.ini** file by adding **log_warnings=2** to **[mysqld]**.
- For a Linux OS, modify the **my.conf** file by adding **log_warnings=2** to **[mysqld]**.

----End

Filezilla

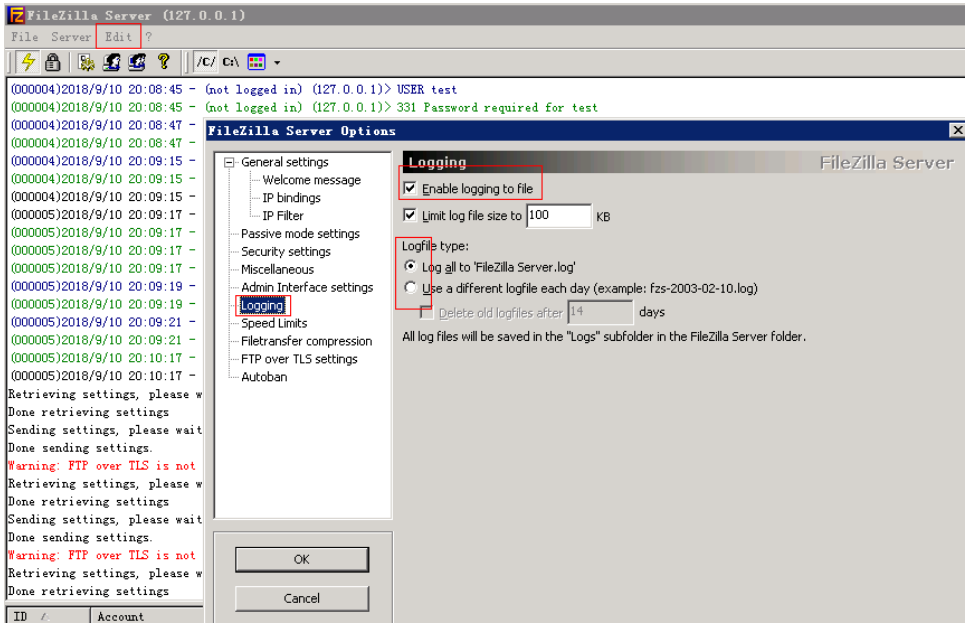
In the account cracking prevention function of HSS, only Windows OSs support FileZilla 0.9.60. Logging is disabled in FileZilla by default.

To enable the logging function, perform the following steps:

Step 1 Open FileZilla.

Step 2 Choose **Edit** > **Settings** > **Logging** and select **Enable logging to file** (see **Figure 14-14**).

Figure 14-14 Enabling logging in FileZilla



----End

vsftp

This section shows you how to enable logging for vsftp login failures.

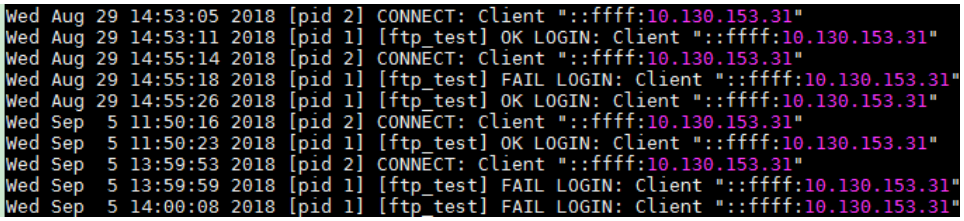
Step 1 Modify the configuration file (for example, **/etc/vsftpd.conf**) and set the following parameters:

vsftpd_log_file=log/file/path

dual_log_enable=YES

Step 2 Restart the vsftp service. If the setting is successful, log records shown in the logs shown in **Figure 14-15** will be returned when you log in to vsftp.

Figure 14-15 Log records



----End

14.6.4 How Do I Scan My Servers?

The HSS service detects risks and abnormal operations on servers in real time and performs a comprehensive scan for the servers every early morning. In addition, you can conduct manual detections to check key configuration information on servers.

The manual detection can detect risky software, vulnerabilities, web shells, weak passwords, and key configurations.

NOTICE

At least a three-minute interval is required between two manual detections for the same item.

Prerequisites

The **Agent Status** of the server is **Online**, the **Protection Status** is **Enabled**, and the **Edition** is **Enterprise** or **Premium**.

Check Items

HSS will scan your servers for software information, Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, web shells, password risks, and unsafe settings configuration.

Scan Duration

- The scan for a single item (such as password risks) takes less than 30 minutes.
- A comprehensive manual scan takes less than 30 minutes. Items are scanned concurrently.

Performing a Manual Detection with One Click

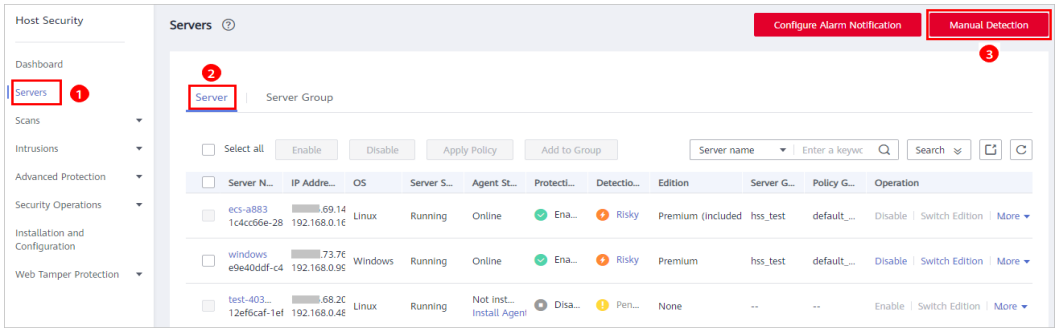
Performing a manual detection with one click can detect risky software information, vulnerabilities, web shells, key configuration information, weak password complexity policies, and accounts using weak passwords on the servers. After the detection is complete, you can view overall risk statistics or the details of a single server 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** > **Host Security Service**.

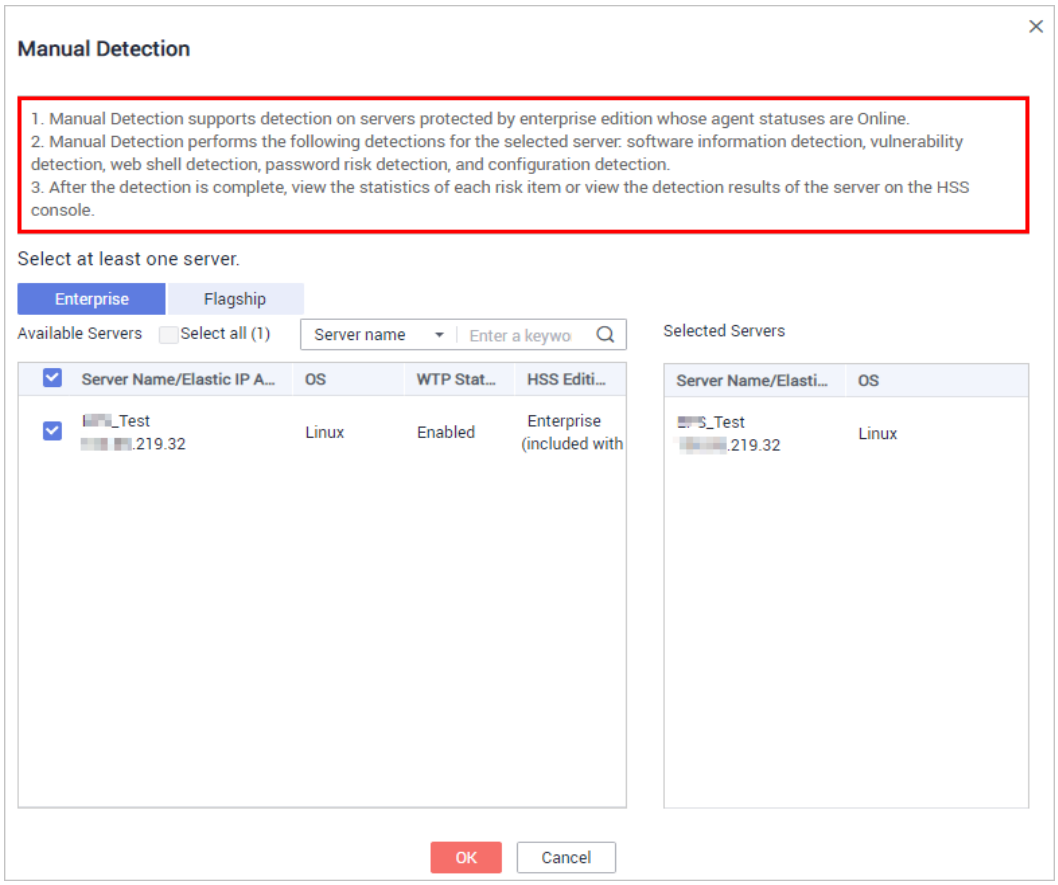
Step 3 In the upper right corner of the **Servers** page, click **Manual Detection**.

Figure 14-16 Performing a manual detection



Step 4 On the **Manual Detection** page, select the target servers and click **OK**.

Figure 14-17 Manual detection



Step 5 On the **Dashboard** page of the HSS console, view the overall detection result. Alternatively, on the **Servers** page, click **View Scan Results** in the **Operation** column of a server to view the manual detection results of the server.

----End

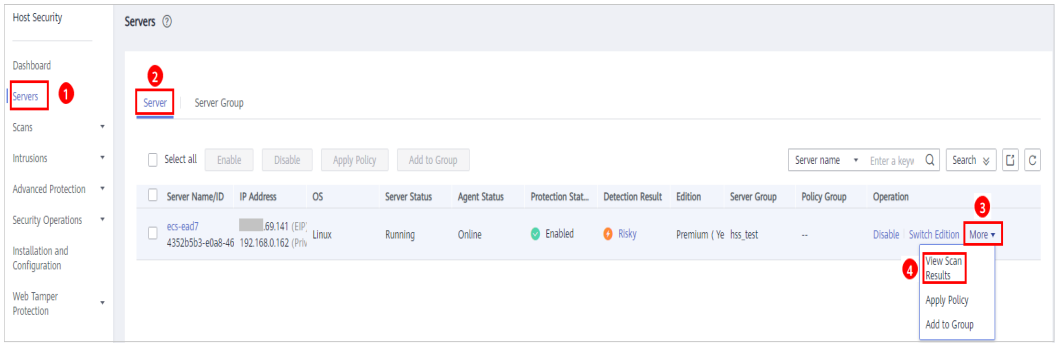
Manually Checking an Item

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** > **Host Security Service**.

Step 3 In the navigation pane, choose **Servers**. In the **Operation** column of the server list, click **View Scan Results**.

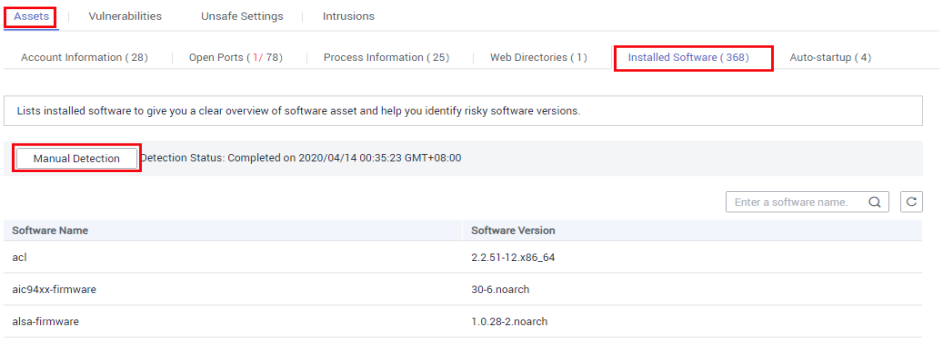
Figure 14-18 Viewing scan results



- **Checking software information**

  Click **Installed Software** on the **Assets** tab, and click **Manual Detection**.

  Figure 14-19 Viewing software information



- **Detecting vulnerabilities**

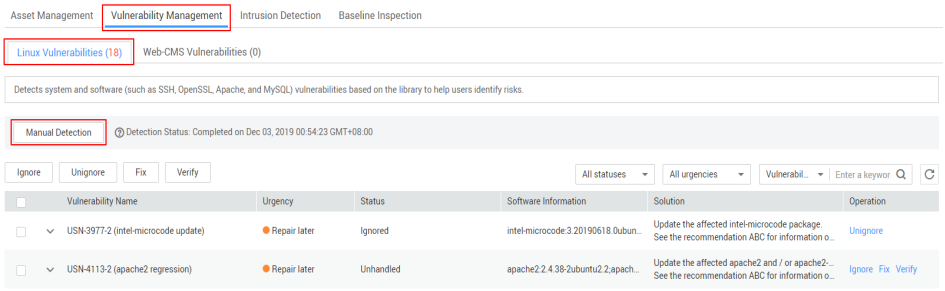
  Click the **Vulnerabilities** tab. Click **Linux Vulnerabilities** or **Web-CMS Vulnerabilities** and click **Manual Detection**.

  NOTE

  The manual detection of either software vulnerabilities or software information management will collect software information from servers.

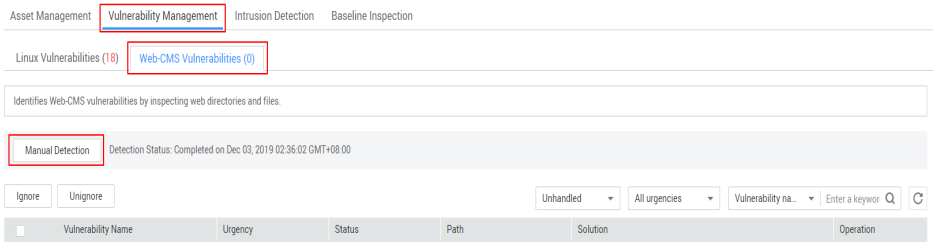
– Click Select the **Vulnerability Management** tab, select a system vulnerability, and click **Manual Detection**. HSS will scan for system vulnerabilities immediately.

Figure 14-20 Detecting system vulnerabilities



– Click the **Vulnerabilities** tab. Click **Web-CMS Vulnerabilities**, select a vulnerability, and click **Manual Detection**. HSS will detect Web-CMS vulnerabilities immediately.

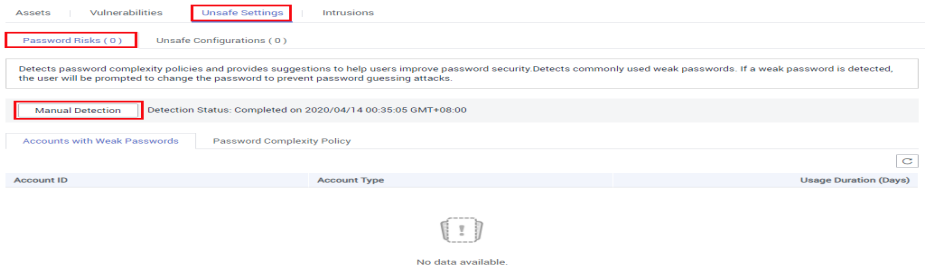
Figure 14-21 Detecting Web-CMS vulnerabilities



- **Detecting password risks**

  Click the **Unsafe Settings** tab and click **Password Risks**. Click **Manual Detection** to manually detect unsafe configurations.

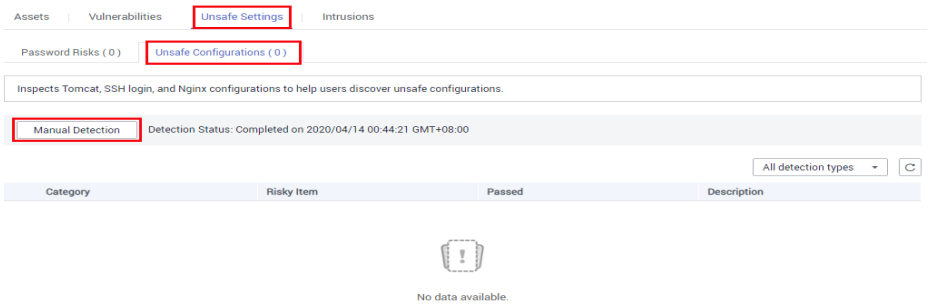
  Figure 14-22 Detecting weak passwords



- **Detecting unsafe settings**

  Click the **Unsafe Settings** tab and click **Unsafe Configurations**. Click **Manual Detection** to manually detect unsafe configurations.

Figure 14-23 Detecting unsafe settings



Step 4 Wait until **Detection Status** changes to **Completed**, click to refresh the detection results.

----End

A Change History

Released On	Description
2021-06-30	This is the second official release. Added section "HSS Permissions Management".
2020-09-30	This is the first official release.