

Host Security Service

User Guide

Issue 01
Date 2024-04-15



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

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Introduction.....	1
1.1 What Is HSS?.....	1
1.2 Advantages.....	4
1.3 Scenarios.....	5
1.4 Editions and Features.....	6
1.5 HSS Permissions Management.....	36
1.6 Constraints and Limitations.....	37
1.7 Basic Concepts.....	40
2 Enabling HSS.....	42
2.1 Installing an Agent.....	42
2.1.1 Installing an Agent on Linux.....	42
2.1.2 Installing an Agent on Windows.....	43
2.2 Enabling HSS.....	45
2.2.1 Enabling the Enterprise/Premium Edition.....	45
2.2.2 Enabling the WTP Edition.....	49
2.3 Enabling Container Node Protection.....	51
2.4 (Optional) Switching the HSS Edition.....	52
2.5 Installation and Configuration.....	53
3 Server Security Dashboard.....	58
3.1 Risk Statistics.....	58
4 Asset Management.....	61
4.1 Asset Management.....	61
4.2 Server Fingerprints.....	61
4.2.1 Viewing Server Asset Fingerprints.....	61
4.2.2 Viewing the Operation History of Server Assets.....	65
4.2.3 Manually Updating Server Asset Information in Real Time.....	66
4.3 Container Fingerprints.....	66
4.3.1 Viewing Container Asset Fingerprints.....	67
4.3.2 Manually Updating Container Asset Information in Real Time.....	74
4.4 Server Management.....	75
4.4.1 Viewing Server Protection Status.....	75
4.4.2 Enabling Protection.....	77

4.4.2.1 Enterprise/Premium Edition.....	77
4.4.2.2 WTP Edition.....	79
4.4.3 Disabling Protection.....	80
4.4.3.1 Enterprise/Premium Edition.....	80
4.4.3.2 WTP Edition.....	81
4.4.4 Applying a Policy.....	82
4.4.5 Managing Server Groups.....	83
4.4.6 Configuring Asset Importance.....	85
4.5 Container Management.....	86
4.5.1 Viewing the Clusters and Protection Quotas.....	86
4.5.2 Enabling Container Security Protection.....	87
4.5.3 Disabling Container Security Protection.....	88
4.5.4 Container Images.....	89
4.5.4.1 Local Images.....	89
4.5.5 Viewing Container Information.....	91
4.5.6 Handling Risk Containers.....	92
5 Risk Prevention.....	94
5.1 Vulnerability Management.....	94
5.1.1 Vulnerability Management Overview.....	94
5.1.2 Vulnerability Scan.....	97
5.1.3 Viewing Vulnerability Details.....	99
5.1.4 Fixing and Verifying the Fix of Vulnerabilities.....	102
5.1.5 Managing the Vulnerability Whitelist.....	109
5.1.6 Viewing Vulnerability Handling History.....	112
5.2 Baseline Inspection.....	113
5.2.1 Baseline Check Overview.....	113
5.2.2 Viewing Baseline Check Details.....	116
5.2.3 Fixing Unsafe Settings.....	120
5.2.4 Managing Baseline Check Policies.....	124
5.3 Container Image Security.....	126
5.3.1 Image Vulnerabilities.....	126
5.3.2 Viewing Malicious File Detection Results.....	127
5.3.3 Image Baseline Check.....	128
6 Prevention.....	130
6.1 Application Protection.....	130
6.1.1 Viewing Application Protection.....	130
6.1.2 Enabling Application Protection.....	132
6.1.3 Managing Application Protection.....	133
6.1.4 Disabling Application Protection.....	133
6.1.5 Managing Policies.....	134
6.2 WTP.....	137
6.2.1 Adding a Protected Directory.....	137

6.2.2 Managing Remote Backup Servers.....	141
6.2.3 Setting Scheduled WTP Protection.....	143
6.2.4 Enabling Dynamic WTP.....	144
6.2.5 Viewing WTP Reports.....	144
6.2.6 Viewing WTP Events.....	145
6.2.7 Adding a Privileged Process.....	145
6.3 Ransomware Prevention.....	147
6.3.1 Purchasing a Backup Vault.....	147
6.3.2 Enabling Ransomware Prevention.....	148
6.3.3 Preventing Ransomware.....	153
6.3.4 Disabling Ransomware Prevention.....	161
6.3.5 Managing Protection Policies.....	161
6.4 File Integrity Monitoring.....	165
6.4.1 Viewing File Integrity Management.....	165
6.4.2 Checking Change Details.....	165
6.4.3 Checking Modified Files.....	166
7 Intrusion Detection.....	167
7.1 Alarms.....	167
7.1.1 HSS Alarms.....	167
7.1.1.1 Server Alarms.....	167
7.1.1.2 Viewing Intrusion Alarms.....	179
7.1.1.3 Managing Isolated Files.....	181
7.1.1.4 Handling Server Alarms.....	183
7.1.2 Container Alarms.....	186
7.1.2.1 Container Alarm Events.....	187
7.1.2.2 Viewing Container Alarms.....	191
7.1.2.3 Handling Container Alarms.....	192
7.2 Whitelist Management.....	194
7.2.1 Configuring the Login Whitelist.....	194
7.2.2 Managing the Alarm Whitelist.....	195
7.2.3 Configuring the System User Whitelist.....	197
8 Security Operations.....	199
8.1 Policy Management.....	199
8.1.1 Viewing a Policy Group.....	199
8.1.2 Creating a Policy Group.....	206
8.1.3 Modifying a Policy.....	208
8.2 Viewing the Handling History.....	226
9 Security Report.....	228
9.1 Checking a Security Report.....	228
9.2 Subscribing to a Security Report.....	229
9.3 Creating a Security Report.....	230

9.4 Managing a Security Report.....	231
10 Installation & Configuration.....	234
10.1 Agent Management.....	234
10.1.1 Viewing Agent Management.....	234
10.1.2 Installing an Agent.....	234
10.1.3 Uninstalling an Agent.....	236
10.1.4 Upgrading the Agent.....	239
10.2 Security Configurations.....	241
10.3 Plug-in Management.....	241
10.3.1 Plug-Ins Overview.....	241
10.3.2 Viewing Plug-in Details.....	241
10.3.3 Installing a Plug-in.....	243
10.3.4 Upgrading a Plug-in.....	244
10.3.5 Uninstalling a Plug-in.....	245
11 Permissions Management.....	247
11.1 Creating a User and Granting Permissions.....	247
11.2 HSS Custom Policies.....	249
12 FAQs.....	251
12.1 About HSS.....	251
12.1.1 What Is HSS?.....	251
12.1.2 What Is Container Security Service?.....	252
12.1.3 What Is Web Tamper Protection?.....	252
12.1.4 What Are the Relationships Between Images, Containers, and Applications?.....	254
12.1.5 How Do I Use HSS?.....	255
12.1.6 Can HSS Protect Local IDC Servers?	255
12.1.7 Is HSS in Conflict with Any Other Security Software?	255
12.1.8 What Are the Differences Between HSS and WAF?.....	255
12.1.9 What Is the HSS Agent?.....	256
12.2 Agent FAQs.....	257
12.2.1 Is the Agent in Conflict with Any Other Security Software?.....	257
12.2.2 How Do I Install the Agent?.....	257
12.2.3 How Do I Uninstall the Agent?.....	257
12.2.4 What Should I Do If Agent Installation Failed?.....	259
12.2.5 How Do I Fix an Abnormal Agent?.....	260
12.2.6 What Is the Default Agent Installation Path?.....	261
12.2.7 How Many CPU and Memory Resources Are Occupied by the Agent When It Performs Scans?....	261
12.2.8 Do WTP and HSS Use the Same Agent?.....	262
12.2.9 How Do I View Servers Where No Agents Have Been Installed?.....	263
12.3 Brute-force Attack Defense.....	263
12.3.1 How Does HSS Intercept Brute Force Attacks?.....	263
12.3.2 How Do I Handle a Brute-force Attack Alarm?.....	265

12.3.3 How Do I Defend Against Brute-force Attacks?.....	268
12.3.4 How Do I Do If the Account Cracking Prevention Function Does Not Take Effect on Some Linux Accounts?.....	269
12.3.5 How Do I Unblock an IP Address?.....	270
12.3.6 What Do I Do If HSS Frequently Reports Brute-force Alarms?	271
12.3.7 What Do I Do If My Remote Server Port Is Not Updated in Brute-force Attack Records?.....	272
12.4 Weak Passwords and Unsafe Accounts.....	272
12.4.1 How Do I Handle a Weak Password Alarm?.....	272
12.4.2 How Do I Set a Secure Password?.....	274
12.4.3 Why Are the Weak Password Alarms Still Reported After the Weak Password Policy Is Disabled?	275
12.5 Intrusions.....	276
12.5.1 What Do I Do If My Servers Are Subjected to a Mining Attack?.....	276
12.5.2 Why a Process Is Still Isolated After It Was Whitelisted?.....	279
12.5.3 What Do I Do If a Mining Process Is Detected on a Server?.....	280
12.5.4 Why Some Attacks on Servers Are Not Detected?.....	280
12.5.5 Can I Unblock an IP Address Blocked by HSS, and How?.....	280
12.5.6 Why a Blocked IP Address Is Automatically Unblocked?.....	281
12.5.7 How Often Does HSS Detect, Isolate, and Kill Malicious Programs?	281
12.5.8 What Do I Do If an IP Address Is Blocked by HSS?	281
12.5.9 How Do I Defend Against Ransomware Attacks?	281
12.6 Abnormal Logins.....	282
12.6.1 Why Do I Still Receive Remote Login Alarms After Configuring the Login IP Whitelist?.....	282
12.6.2 How Do I Check the User IP address of a Remote Login?.....	282
12.6.3 How Do I Know Whether an Intrusion Succeeded?.....	283
12.7 Unsafe Settings.....	283
12.7.1 How Do I Install a PAM and Set a Proper Password Complexity Policy in a Linux OS?.....	283
12.7.2 How Do I Set a Proper Password Complexity Policy in a Windows OS?.....	285
12.7.3 How Do I Handle Unsafe Configurations?.....	286
12.7.4 How Do I View Configuration Check Reports?.....	286
12.8 Vulnerability Management.....	287
12.8.1 How Do I Fix Vulnerabilities?.....	287
12.8.2 What Do I Do If an Alarm Still Exists After I Fixed a Vulnerability?.....	287
12.8.3 Why a Server Displayed in Vulnerability Information Does Not Exist?.....	288
12.8.4 Do I Need to Restart a Server After Fixing its Vulnerabilities?.....	288
12.8.5 Can I Check the Vulnerability and Baseline Fix History on HSS?	288
12.9 Web Tamper Protection.....	289
12.9.1 Why Do I Need to Add a Protected Directory?.....	289
12.9.2 How Do I Modify a Protected Directory?.....	289
12.9.3 What Should I Do If WTP Cannot Be Enabled?.....	290
12.9.4 How Do I Modify a File After WTP Is Enabled?.....	290
12.9.5 What Can I Do If I Enabled Dynamic WTP But Its Status Is Enabled but not in effect?.....	291
12.9.6 What Are the Differences Between the Web Tamper Protection Functions of HSS and WAF?.....	291

12.10 Container Guard Service.....	292
12.10.1 How Do I Disable Node Protection?	293
12.10.2 What Is the Log Processing Mechanism of CGS?.....	294
12.10.3 How Do I Enable Node Protection?.....	294
12.10.4 How Do I Enable the API Server Audit for an On-Premises Kubernetes Container?.....	294
12.11 Ransomware Protection.....	297
12.11.1 What Are the Differences Between Ransomware Protection Backup and Cloud Backup?.....	297
12.12 Security Configurations.....	297
12.12.1 How Do I Clear the SSH Login IP Address Whitelist Configured in HSS?	297
12.12.2 What Can I Do If I Cannot Remotely Log In to a Server via SSH?	298
12.12.3 How Do I Use 2FA?	298
12.12.4 What Do I Do If I Cannot Enable 2FA?	299
12.12.5 Why Can't I Receive a Verification Code After 2FA Is Enabled?	300
12.12.6 Why Does My Login Fail After I Enable 2FA?	301
12.12.7 How Do I Add a Mobile Phone Number or Email Address for Receiving 2FA Verification Notifications?	302
12.12.8 If I Choose to Use Verification Code for 2FA, How Do I Get the Code?	302
12.12.9 How Do I Disable the SELinux Firewall?.....	302
12.13 Quotas.....	303
12.13.1 How Do I Filter Unprotected Servers?.....	303
12.13.2 What Do I Do If My Quotas Are Insufficient and I Failed to Enable Protection?	304
12.13.3 If I Change the OS of a Protected Server, Does It Affect My HSS Quota?.....	304
12.14 Others.....	306
12.14.1 How Do I Use the Windows Remote Desktop Connection Tool to Connect to a Server?.....	306
12.14.2 How Do I Check HSS Log Files?.....	306
12.14.3 How Do I Enable Logging for Login Failures?.....	307
12.14.4 How Do I Clear an Alarm on Critical File Changes?.....	308
12.14.5 Is HSS Available as Offline Software?.....	308
12.14.6 How Do I Enable HSS Self-Protection?.....	308
12.14.7 What Do I Do If HSS Self-Protection Cannot Be Disabled?.....	309
A Change History.....	311

1 Introduction

1.1 What Is HSS?

HSS is designed to protect server workloads in hybrid clouds and multi-cloud data centers. It provides host security functions, Container Guard Service (CGS), and Web Tamper Protection (WTP).

HSS can help you remotely check and manage your servers and containers in a unified manner.

HSS protects your system integrity, enhances application security, monitors user operations, and detects intrusions.

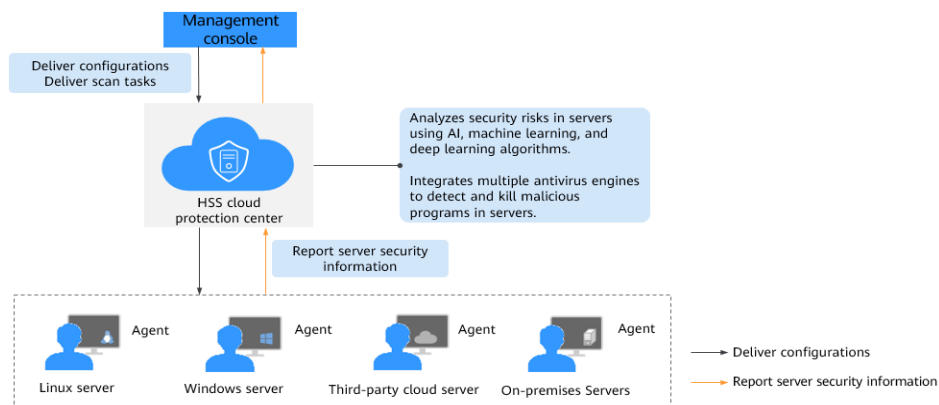
Host Security

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.

Install the HSS agent on your servers, and you will be able to check the server protection 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 the 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 protection status and scan results of servers in a region.
HSS cloud protection center	<ul style="list-style-type: none"> Analyzes security risks in servers using AI, machine learning, and deep learning algorithms. 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	<ul style="list-style-type: none">• Communicates with the HSS cloud protection center via HTTPS and WSS. Port 10190 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. <p>NOTE</p> <ul style="list-style-type: none">• If no agent is installed or the agent installed is abnormal, the HSS is unavailable.• Select the agent and installation command suitable for your OS.• The HSS agent can be used for all editions, including container security and Web Tamper Protection (WTP). You only need to install the agent once on the same server.

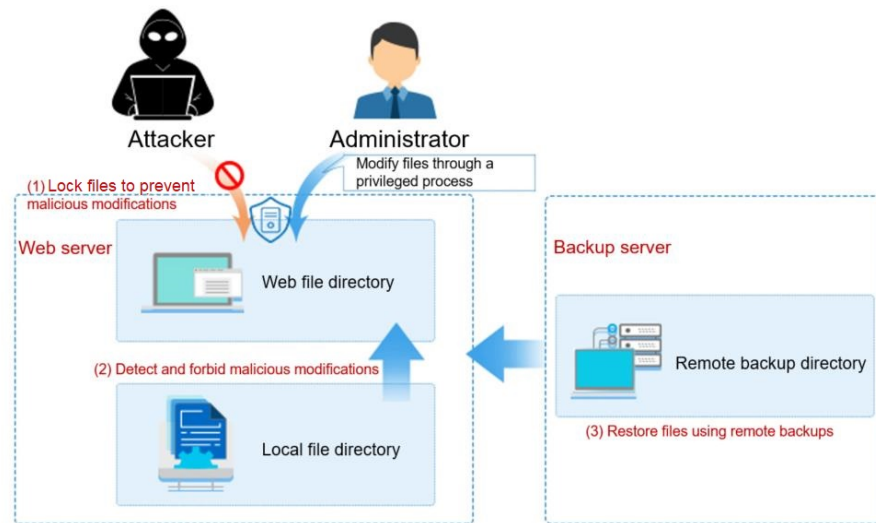
Container Security

HSS provides container security capabilities. The agent deployed on a server can scan the container images on the server, checking configurations, detecting vulnerabilities, and uncovering runtime issues that cannot be detected by traditional security software. Container security also provides functions such as process whitelist, read-only file protection, and container escape detection to minimize the security risks for a running container.

Web Tamper Protection

Web Tamper Protection (WTP) monitors website directories in real time and restores tampered files and directories using their backups. It protects website information, such as web pages, electronic documents, and images, from being tampered with or damaged by hackers.

Figure 1-2 How WTP works



1.2 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.

- You can install the agent on ECSs in the same region to manage them all on a single console.
- 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.

WTP

- The third-generation web anti-tampering technology and kernel-level event triggering technology are used. Files in user directories can be locked to prevent unauthorized tampering.
- The tampering detection and recovery technologies are used. Files modified only by authorized users are backed up on local and remote servers in real time, and will be used to recover tampered websites (if any) detected by HSS.

1.3 Scenarios

HSS

- DJCP Multi-level Protection Scheme (MLPS) compliance
The intrusion detection function of HSS protects accounts and systems on cloud servers, helping companies meet compliance standards.
To apply for the DJCP MLPS certification, purchase the enterprise edition or a higher edition (premium edition or Web Tamper Protection edition).
- Centralized security management
With HSS, you can manage the security configurations and events of all your cloud servers on the 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.

CGS

- Container image security
Vulnerabilities will probably be introduced to your system through the images downloaded from Docker Hub or through open-source frameworks.
You can use CGS to scan images for risks, including image vulnerabilities, unsafe accounts, and malicious files. Receive reminders and suggestions and eliminate the risks accordingly.
- Container runtime security

Develop a whitelist of container behaviors to ensure that containers run with the minimum permissions required, securing containers against potential threats.

- Compliance with DJCP MLPS

Prevent intrusions and malicious code, making sure your container and system security meet compliance requirements.

1.4 Editions and Features

HSS comes in the enterprise, premium, Web Tamper Protection (WTP), and container security editions, providing asset management, vulnerability management, baseline check, intrusion detection, web tamper protection, and container image security functions. For details about the features of the editions, see [Edition Details](#).

Features

HSS provides asset management, baseline check, and intrusion detection features, enhancing server security in all aspects. For details about the features of different editions, see [Edition Details](#).

Table 1-2 HSS functions and features

Feature	Description
Asset management	Provide centralized asset overview, asset fingerprint management, server management, and container management. You can check your asset running status, asset fingerprints, and asset types; and manage assets by server or container.
Vulnerability management	Detect vulnerabilities and risks in Linux, Windows, Web content management systems (Web-CMS), and applications.
Baseline check	Scan for unsafe settings, weak passwords, and password complexity policies in server OS and key software. A security practice baseline and a compliance standard baseline can be used for scans. You can customize baseline sub-items used in scan. You can repair and verify the detected risks.
Container image security	Scan the images that are running or displayed in your image list, and provide suggestions on how to fix vulnerabilities and malicious files.
Application protection	Protect running applications. You simply need to add probes to applications, without having to modify application files. Currently, only Linux servers are supported, and only Java applications can be connected.

Feature	Description
Web page tampering prevention	Detect and prevent tampering of files in specified directories, including web pages, documents, and images, and quickly restore them using valid backup files.
File integrity monitoring	Check the files in the Linux OS, applications, and other components to detect tampering.
Intrusion detection	Identify and prevent intrusion to servers, discover risks in real time, detect and kill malicious programs, and identify web shells and other threats.
Container intrusion detection	Scan running containers for malicious programs including miners and ransomware; detect non-compliant security policies, file tampering, and container escape; and provide suggestions.
Whitelist management	To reduce false alarms, import events to and export events from the whitelist. Whitelisted events will not trigger alarms.
Policy management	You can group policies and servers to batch apply policies to servers, easily adapting to your business scenarios.
Handling history	Check historical vulnerability handling records, including the vulnerability handling time and handlers.
Security report	Check weekly or monthly server security trend, key security events, and risks.
Security configuration	Configure common login locations, common login IP addresses, the SSH login IP address whitelist, and automatic isolation and killing of malicious programs.
HSS self-protection	Protect HSS files, processes, and software from malicious programs, which may uninstall HSS agents, tamper with HSS files, or stop HSS processes.

Recommended Editions

- If your servers store important data assets, have high security risks, use publicly available EIPs, or there are databases running on your servers, you are advised to enable the premium or Web Tamper Protection edition.
- For servers that need to protect websites and applications from tampering, the WTP edition is recommended.
- For containers that need to enhance image security, container runtime security, container edition is recommended.

NOTICE

- You are advised to **deploy HSS on all your servers** so that if a virus infects one of them, it will not be able to spread to others and damage your entire network.

Edition Details

Table 1-3 Editions

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
Assets		Collect statistics on asset status and usage of all servers.	√	√	√	√	Linux and Windows	Real-time check
Servers & Quota		Manage all server assets, including their protection status, quotas, and policy allocation.	√	√	√	√	Linux and Windows	-
Containers & Quota		Manage container nodes and images (private image repositories and local images).	×	×	×	√	Linux	-
Asset Fingerprints	Account	Check and manage server accounts all in one place.	√	√	√	√	Linux and Windows	Real-time check
	Open port	Check open ports all in one place and identify high-risk and unknown ports.	√	√	√	√	Linux and Windows	Real-time check
	Process	Check running applications all in one place and identify malicious applications.	√	√	√	√	Linux and Windows	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Installed software	Check and manage server software all in one place and identify insecure versions.	√	√	√	√	Linux and Windows	Automatic check in the early morning every day
	Auto-startup	Check auto-startup entries and collect statistics on entry changes in a timely manner.	√	√	√	√	Linux and Windows	Real-time check
	Web applications	Check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software.	√	√	√	√	Linux and Windows (only Tomcat is supported)	Once a week (05:00 a.m. every Monday)
	Web service	Check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software.	√	√	√	√	Linux	Once a week (05:00 a.m. every Monday)
	Web framework	Check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	√	√	√	√	Linux	Once a week (05:00 a.m. every Monday)

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Websites check	Check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, and key processes of websites.	√	√	√	√	Linux	Once a week (05:00 a.m. every Monday)
	Middleware	Check information about servers, versions, paths, and processes associated with middleware.	√	√	√	√	Linux	Once a week (05:00 a.m. every Monday)
	Database	Check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software.	√	√	√	√	Linux and Windows (only MySQL is supported)	Once a week (05:00 a.m. every Monday)

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
Vulnerability Management	Linux vulnerability detection	Based on the vulnerability database, check and handle vulnerabilities in the software (such as kernel, OpenSSL, vim, glibc) you obtained from official Linux sources and have not compiled.	√	√	√	√	Linux	<ul style="list-style-type: none"> • Automatic check in the early morning every day • Manual scan
	Windows vulnerability detection	Detect vulnerabilities in Windows OS based on the official patch releases of Microsoft.	√	√	√	√	Windows	<ul style="list-style-type: none"> • Automatic check in the early morning every day • Manual scan

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Web-CMS vulnerability detection	Scan for Web-CMS vulnerabilities in web directories and files.	√	√	√	√	Linux and Windows	<ul style="list-style-type: none"> Automatic check in the early morning every day Manual scan
	Application vulnerability detection	Detect vulnerabilities in JAR packages, ELF files, and other files of open source software, such as Log4j and spring-core.	√	√	√	√	Linux and Windows	<ul style="list-style-type: none"> Once a week (05:00 a.m. every Monday) Manual scan

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
Unsafe settings check	Password policy check	Check password complexity policies and modify them based on suggestions provided by HSS to improve password security.	√	√	√	√	Linux	<ul style="list-style-type: none"> • Automatic check in the early morning every day • Manual scan
	Weak password check	Change weak passwords to stronger ones based on HSS scan results and suggestions.	√	√	√	√	Linux	<ul style="list-style-type: none"> • Automatic check in the early morning every day • Manual scan

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Unsafe configurations	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.	√	√	√	√	Linux and Windows	<ul style="list-style-type: none"> • Automatic check in the early morning every day • Manual scan
Container image security	Container image vulnerability management	Detect and manage vulnerabilities in local images and private image repositories based on a vulnerability database, and handle critical vulnerabilities in a timely manner.	×	×	×	√	Linux	<ul style="list-style-type: none"> • Automatic check in the early morning every day • Manual scan

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Malicious image file detection	Scan images for malicious files (such as Trojans, worms, viruses, and adware) and identify risks.	×	×	×	√	Linux	Real-time check
	Image baseline check	Check for insecure configurations based on 18 types of container baselines.	×	×	×	√	Linux	Real-time check
Application protection	SQL injection	Detect and defend against SQL injection attacks, and check web applications for related vulnerabilities.	×	√	√	√	Linux	Real-time check
	OS command injection	Detect and defend against remote OS command injection attacks and check web applications for related vulnerabilities.	×	√	√	√	Linux	Real-time check
	XSS	Detect and defend against stored cross-site scripting (XSS) injection attacks.	×	√	√	√	Linux	Real-time check
	Log4j RCE vulnerability	Detect and defend against remote code execution.	×	√	√	√	Linux	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Web shell upload	Detect and defend against attacks that upload dangerous files, change file names, or change file name extension types; and check web applications for related vulnerabilities.	×	√	√	√	Linux	Real-time check
	XXE attack	Detect and defend against XML External Entity Injection (XXE) attacks, and check web applications for related vulnerabilities.	×	√	√	√	Linux	Real-time check
	Deserialization input	Detect deserialization attacks that exploit unsafe classes.	×	√	√	√	Linux	Real-time check
	File directory traversal	Check whether sensitive directories or files are accessed.	×	√	√	√	Linux	Real-time check
	Struts 2 OGNL	Detect OGNL code execution.	×	√	√	√	Linux	Real-time check
	Command execution using JSP	Detect command execution using JSP.	×	√	√	√	Linux	Real-time checks
	File deletion using JSP	Detects file deletion using JSP.	×	√	√	√	Linux	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Database connection exception	Detect authentication and communication exceptions thrown by database connections.	×	√	√	√	Linux	Real-time check
	0-day vulnerability	Check whether the stack hash of a command is in the whitelist of the web application.	×	√	√	√	Linux	Real-time check
	SecurityManager permission exception	Detect exceptions thrown by SecurityManager.	×	√	√	√	Linux	Real-time check
Web page tampering prevention	Static WTP	Protect the static web page files on your website servers from malicious modification.	×	×	√	×	Linux and Windows	Real-time check
	Dynamic WTP	Protect the dynamic web page files in your website databases from malicious modification.	×	×	√	×	Linux	Real-time check
Ransomware prevention	Ransomware prevention	Help you identify and detect known ransomware attacks and restore services using backups.	×	√	√	√	Linux and Windows	Real-time checks

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
File integrity monitoring	File Integrity	Check the files in the Linux OS, applications, and other components to detect tampering.	×	√	√	√	Linux	Real-time check
Intrusion detection	Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojan, mining software, worms, and viruses.	√	√	√	√	Linux and Windows	Real-time check
	Virus	Check servers in real time and report alarms for viruses detected on servers.	√	√	√	√	Linux and Windows	Real-time check
	Worm	Detect and kill worms on servers and report alarms.	√	√	√	√	Linux and Windows	Real-time check
	Trojan	Detect programs that are hidden in normal programs and have special functions such as damaging and deleting files, sending passwords, and recording keyboards. If a program is detected, an alarm is reported immediately.	√	√	√	√	Linux and Windows	Real-time check
	Botnet	Detect whether zombie programs that have been spread exist in servers and report alarms immediately after detecting them.	√	√	√	√	Linux and Windows	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Web shell	Detect web shell attacks in the server system in real time and report alarms immediately after detecting them.	√	√	√	√	Linux and Windows	Real-time check
	Rootkit	Detect server assets and report alarms for suspicious kernel modules, files, and folders.	√	√	√	√	Linux	Real-time check
	Ransomware	Check ransomware embedded in media such as web pages, software, emails, and storage media. Ransomware is used to encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.	×	√	√	√	Linux and Windows	Real-time check
	Hacker tool	Check whether non-standard tool used to control the server exist and report alarms immediately after detecting them.	√	√	√	√	Linux and Windows	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Web shell	<p>Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells.</p> <ul style="list-style-type: none"> 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. 	√	√	√	√	Linux and Windows	Real-time check
	Mininig	Detect whether mining software exists on servers in real time and report alarms for the detected software.	√	√	√	√	Linux and Windows	Real-time check
	Remote code execution	Check whether the server is remotely called in real time and report an alarm immediately once remote code execution is detected.	√	√	√	√	Linux and Windows	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	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.	√	√	√	√	Linux	Real-time check
	File privilege escalation	Check the file privilege escalations in your system.	√	√	√	√	Linux	Real-time check
	Process privilege escalation	The following process privilege escalation operations can be detected: <ul style="list-style-type: none"> • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities 	√	√	√	√	Linux	Real-time check
	Change in critical file	Receive alarms when critical system files are modified.	√	√	√	√	Linux and Windows	Real-time check
	File/Directory change	System files and directories are monitored. If a file or directory is modified, an alarm is generated, indicating that the file or directory may be tampered with.	√	√	√	√	Linux and Windows	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Abnormal process behavior	<p>Check the processes on servers, including their IDs, command lines, process paths, and behavior.</p> <p>Send alarms on unauthorized process operations and intrusions.</p> <p>The following abnormal process behavior can be detected:</p> <ul style="list-style-type: none"> Abnormal CPU usage Processes accessing malicious IP addresses Abnormal increase in concurrent process connections 	√	√	√	√	Linux and Windows	Real-time check
	High-risk command execution	Receive real-time alarms on high-risk commands.	√	√	√	√	Linux and Windows	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.	√	√	√	√	Linux	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Suspicious cron task	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.	×	√	√	√	Linux and Windows	Real-time check
	System protection disabling	Detect the preparations for ransomware encryption: Disable the Windows defender real-time protection function through the registry. Once the function is disabled, an alarm is reported immediately.	√	√	√	×	Windows	Real-time check
	Backup deletion	Detect the preparations for ransomware encryption: Delete backup files or files in the Backup folder. Once backup deletion is detected, an alarm is reported immediately.	√	√	√	√	Windows	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Suspicious registry operation	Detect operations such as disabling the system firewall through the registry and using the ransomware Stop to modify the registry and write specific strings in the registry. An alarm is reported immediately when such operations are detected.	√	√	√	√	Windows	Real-time check
	System log deletion	An alarm is generated when a command or tool is used to clear system logs.	√	√	√	×	Windows	Real-time check
	Suspicious command execution	<ul style="list-style-type: none"> Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. Detect suspicious remote command execution. 	√	√	√	×	Windows	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Brute-force attack defense	<p>Check for brute-force attack attempts and successful brute-force attacks.</p> <ul style="list-style-type: none"> Your accounts are protected from brute-force attacks. HSS will block the attacking servers when detecting such attacks. Trigger an alarm if a user logs in to the server by a brute-force attack. 	√	√	√	√	Linux and Windows	Real-time check
	Abnormal login	<p>Check and handle remote logins.</p> <p>If a user's login location is not any common login location you set, an alarm will be triggered.</p>	√	√	√	√	Linux and Windows	Real-time check
	Invalid account	<p>Scan accounts on servers and list suspicious accounts in a timely manner.</p>	√	√	√	√	Linux and Windows	Real-time check
	User account added	<p>Detect the commands used to create hidden accounts. Hidden accounts cannot be found in the user interaction interface or be queried by commands.</p>	√	√	√	√	Windows	Real-time check
	Password theft	<p>Detect the abnormal obtaining of hash value of system accounts and passwords on servers and report alarms.</p>	√	√	√	√	Windows	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Suspicious download request	An alarm is generated when a suspicious HTTP request that uses system tools to download programs is detected.	√	√	√	×	Windows	Real-time check
	Suspicious HTTP request	An alarm is generated when a suspicious HTTP request that uses a system tool or process to execute a remote hosting script is detected.	√	√	√	×	Windows	Real-time check
	Port scan	Detect scanning or sniffing on specified ports and report alarms.	×	√	√	√	Linux	Real-time check
	Host scan	Detect the network scan activities based on server rules (including ICMP, ARP, and nbtscan) and report alarms.	×	√	√	√	Linux	Real-time check
Container intrusion detection	Unclassified malware	Check and handle malicious programs in a container, including web shells, Trojan, mining software, worms, and viruses.	×	×	×	√	Linux	Real-time check
	Ransomware	Check and handle alarms on ransomware in containers.	×	×	×	√	Linux	Real-time check
	Web shell	Check whether the files (often PHP and JSP files) in the web directories on containers are web shells.	×	×	×	√	Linux	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Vulnerability escape	An escape alarm is reported if a container process behavior that matches the behavior of known vulnerabilities is detected.	×	×	×	√	Linux	Real-time checks
	File escape	An alarm is reported if a container process is found accessing a key file directory (for example, /etc/shadow or /etc/crontab). Directories that meet the container directory mapping rules can also trigger such alarms.	×	×	×	√	Linux	Real-time 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.	×	×	×	√	Linux	Real-time check
	Process privilege escalation	The following process privilege escalation operations can be detected: <ul style="list-style-type: none"> • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities 	×	×	×	√	Linux	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	High-risk command execution	Check executed commands in containers and generate alarms if high-risk commands are detected.	×	×	×	√	Linux	Real-time check
	Abnormal container process	<ul style="list-style-type: none"> Malicious container program Monitor container process behavior and process file fingerprints. An alarm is reported if it detects a process whose behavior characteristics match those of a predefined malicious program. Abnormal process An alarm is reported if a process not in the whitelist is running in the container. 	×	×	×	√	Linux	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Abnormal container startup	<p>The service monitors container startups and reports an alarm if it detects that a container with too many permissions is started.</p> <p>Container check items include:</p> <ul style="list-style-type: none"> Privileged container startup (privileged:true) Too many container capabilities (capability:[xxx]) Seccomp not enabled (seccomp=unconfined) Container privilege escalation (no-new-privileges:false) High-risk directory mapping (mounts:[...]) 	×	×	×	√	Linux	Real-time check
	High-risk system call	You can run tasks in kernels by Linux system calls. The container edition reports an alarm if it detects a high-risk call.	×	×	×	√	Linux	Real-time check
	Sensitive file accesses	The service monitors the container image files associated with file protection policies, and reports an alarm if the files are modified.	×	×	×	√	Linux	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Container Image blocking	If a container contains insecure images specified in , an alarm will be generated and the insecure images will be blocked before a container is started in Docker. NOTE You need to .	×	×	×	√	Linux	Real-time check
	Brute-force attack	Detect and report alarms for brute-force attack behaviors, such as brute-force attack attempts and successful brute-force attacks, on containers. Detect SSH, web, and Enumdb brute-force attacks on containers. NOTE Currently, brute-force attacks can be detected only in the Docker runtime.	×	×	×	√	Linux	Real-time check
	Invalid system user account	Detect suspicious accounts and report alarms.	×	×	×	√	Linux	Real-time check
	Abnormal pod behavior	Detect abnormal operations such as creating privileged pods, static pods, and sensitive pods in a cluster and abnormal operations performed on existing pods and report alarms.	×	×	×	√	Linux	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	User information enumeration	Detect the operations of enumerating the permissions and executable operation list of cluster users and report alarms.	×	×	×	√	Linux	Real-time check
	Cluster role binding	Detect operations such as binding or creating a high-privilege cluster role or service account and report alarms.	×	×	×	√	Linux	Real-time check
	Kubernetes event deletion	Detect the deletion of Kubernetes events and report alarms.	×	×	×	√	Linux	Real-time check
Whitelist management	Alarm whitelist	You can add an alarm to the whitelist when handling it.	√	√	√	√	Linux and Windows	Real-time check
	Login whitelist	Some alarms can be added to the alarm whitelist.	√	√	√	√	Linux and Windows	Real-time check
	System user whitelist	Users (non-root users) that are newly added to the root user group on a server can be added to the system user whitelist. HSS will not report risky account alarms for them.	√	√	√	√	Linux and Windows	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
Policy management	Querying and editing rule configurations	<p>You can define and issue different detection policies for different servers or server groups, implementing refined security operations.</p> <ul style="list-style-type: none"> 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 & Quota page. 	√ (Only the default enterprise policy group is supported.)	√	√	√	Linux and Windows	Real-time check
Handling history	Vulnerability handling history	Check historical vulnerability handling records, including the vulnerability handling time and handler.	√	√	√	√	Linux and Windows	-
Security report	Server security report	Check weekly or monthly server security trend, key security events, and risks.	√	√	√	√	Linux and Windows	-

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
Security configuration	Agent management	You can view the agent status of all servers and upgrade, uninstall, and install agents.	√	√	√	√	Linux and Windows	Real-time check
	Common login location	For each server, you can configure the locations where users usually log in from. The service will generate alarms on logins originated from locations other than the configured common login locations. A server can be added to multiple login locations.	√	√	√	√	Linux and Windows	Real-time check
	Common login IP address	For each server, you can configure the IP addresses where users usually log in from. The service will generate alarms on logins originated from IP addresses other than the configured common IP addresses.	√	√	√	√	Linux and Windows	Real-time check
	Configuring an SSH login IP address whitelist	The SSH login whitelist controls SSH access to servers to prevent account cracking. After you configure the whitelist, SSH logins will be allowed only from whitelisted IP addresses.	√	√	√	√	Linux	Real-time check

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
	Malicious program isolation and removal	HSS automatically isolates and kills identified malicious programs, such as web shells, Trojans, and worms, removing security risks.	√	√	√	√	Linux and Windows	Real-time check
	2FA	Prevent brute-force attacks by using password and SMS/email authentication.	√	√	√	√	Linux and Windows	-

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
HSS self-protection	HSS self-protection	<p>Protect HSS files, processes, and software from malicious programs, which may uninstall HSS agents, tamper with HSS files, or stop HSS processes.</p> <ul style="list-style-type: none"> • Self-protection depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled. • Enabling the self-protection policy has the following impacts: <ul style="list-style-type: none"> - The HSS agent cannot be uninstalled on the control panel of a server, but can be uninstalled on the HSS console. - HSS process cannot be terminated. - In the agent installation path C:\Program Files\HostGuard, you can only access the log and data directories (and the upgrade 	×	√	√	×	Windows	-

Function	Item	Description	Enterprise Edition	Premium	WTP	Container Edition	Supported OS	Check Frequency
		directory, if your agent has been upgraded).						

1.5 HSS Permissions Management

If you need to assign different permissions to employees in your enterprise to access your HSS resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure the access to your cloud resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. 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 their groups and can perform specified operations on cloud services.

HSS is a project-level service deployed and accessed in specific physical regions. To assign HSS 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 permissions by using roles or policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. Some roles depend on other roles to take effect. When you assign such roles to users, remember to assign the roles they depend on. However, roles are not an ideal choice for fine-grained authorization and secure access control.

- **Policies:** A type of fine-grained authorization that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and ideal for secure access control. For example, you can grant HSS users only the permissions for managing a certain type of resources.

The following table describes more details.

Table 1-4 System-defined permissions supported by HSS

Role/Policy Name	Description	Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS	System-defined role	<ul style="list-style-type: none">• It depends on the Tenant Guest role. Tenant Guest: A global role, which must be assigned in the global project.
HSSFullAccess	All HSS permissions	Policy	None
HSSReadOnlyAccess	Read-only permission for HSS	Policy	None

1.6 Constraints and Limitations

Supported Server Types

- ECS
- Third-party cloud server
- On-premises server

Supported OSs

HSS uses the agent to monitor security risks and defend against external intrusions. To protect a server with HSS, ensure the agent is up and running on the server. For more information, see [Table 1-5](#).

NOTICE

- The agent is probably incompatible with the Linux or Windows 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 1-5 Server OSs supported by the agent

OS Type	System Architecture	Supported OS
Windows	X86	<ul style="list-style-type: none">• Windows Server 2019 Datacenter 64-bit English (40 GB)• Windows Server 2019 Datacenter 64-bit Chinese (40 GB)• Windows Server 2016 Standard 64-bit English (40 GB)• Windows Server 2016 Standard 64-bit Chinese (40 GB)• Windows Server 2016 Datacenter 64-bit English (40 GB)• Windows Server 2016 Datacenter 64-bit Chinese (40 GB)• Windows Server 2012 R2 Standard 64-bit English (40 GB)• Windows Server 2012 R2 Standard 64-bit Chinese (40 GB)• Windows Server 2012 R2 Datacenter 64-bit English (40 GB)• Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB) <p>NOTE 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.</p>
Linux	X86	<ul style="list-style-type: none">• CentOS 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8, 9 (64-bit)• Debian 9, 10, 11.0.0, 11.1.0 (64-bit)• EulerOS 2.2, 2.3, 2.5, 2.7 and 2.9 (64-bit)• Fedora 28 (64-bit)• Ubuntu 16, 18, 20.03, 20.04, 22.04 (64-bit)• Red Hat 7.4, 7.6, 8.0, 8.7 (64-bit)• OpenEuler 20.03 LTS, 22.03 SP3 LTS, 22.03 (64-bit)• AlmaLinux 9.0 (64-bit)• Rocky Linux 8.4, 8.5 and 9.0 (64-bit)• HCE 2.0 (64-bit)• Suse 12 SP5, 15 SP2, 15.5 (64-bit)

OS Type	System Architecture	Supported OS
	ARM	<ul style="list-style-type: none"> CentOS 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, and 9 (64-bit) EulerOS 2.8 and 2.9 (64-bit) Fedora 29 (64-bit) Ubuntu 18 (64-bit) Kylin V7 and V10 (64-bit) HCE 2.0 (64-bit) UOS V20 (64-bit)

OSs that Support Vulnerability Scan and Fix

HSS can scan for and fix vulnerabilities in the OSs described in [Table 1-6](#).

Table 1-6 OSs that support vulnerability scan and fix

OS Type	Supported OS
Windows	<ul style="list-style-type: none"> Windows Server 2019 Datacenter 64-bit English (40 GB) Windows Server 2019 Datacenter 64-bit Chinese (40 GB) Windows Server 2016 Standard 64-bit English (40 GB) Windows Server 2016 Standard 64-bit Chinese (40 GB) Windows Server 2016 Datacenter 64-bit English (40 GB) Windows Server 2016 Datacenter 64-bit Chinese (40 GB) Windows Server 2012 R2 Standard 64-bit English (40 GB) Windows Server 2012 R2 Standard 64-bit Chinese (40 GB) Windows Server 2012 R2 Datacenter 64-bit English (40 GB) Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)
Linux	<ul style="list-style-type: none"> EulerOS: 2.2, 2.3, 2.5, 2.8, 2.9 (64-bit) CentOS 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 (64-bit) Ubuntu 16.04, 18.04, 20.04 (64-bit) Debian 9 and 10 (64-bit) Kylin V10 (64-bit) UnionTech OS V20 server E and V20 server D (64-bit)

1.7 Basic Concepts

Account Cracking

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

Weak Password

A weak password can be easily cracked.

Malicious Program

A malicious program, such as a web shell, Trojan, 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, Trojans, 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.

Cluster

A cluster consists of one or more ECSs (also known as nodes) in the same subnet. It provides a computing resource pool for running containers.

Node

In CGS, each node corresponds to an ECS. Containers run on nodes.

Image

An image is a special file system. It provides not only programs, libraries, resources, configuration files but also some configuration parameters required for a running container. A Docker image does not contain any dynamic data, and its content remains unchanged after being built.

Container

A container is the instance of an image and can be created, started, stopped, deleted, and suspended.

Security Policy

A security policy indicates the security rule that must be followed for a running container. If a container violates a security policy, a container exception is displayed on the **Runtime Security** page of the CGS management console.

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.

Protection Quota

To protect a server, bind it to an HSS quota.

The quotas of different HSS editions you applied for are displayed on the console.

Example:

- If you have applied for an HSS enterprise edition quota, you can bind it to a server.
- If you have applied for 10 HSS enterprise edition quotas, you can bind them to 10 servers.

2 Enabling HSS

2.1 Installing an Agent

2.1.1 Installing an Agent on Linux

To enable workload protection for cloud servers, install the agent first.

This topic describes how to install the agent on a server running Linux.

 **NOTE**

CentOS 6.x is no longer updated or maintained on the Linux official website, and HSS no longer supports CentOS 6.x or earlier.

Default Installation Path

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

`/usr/local/hostguard/`

Prerequisites

- To install the agent on a server on another cloud, ensure the server runs Linux and can access the Internet.
- The Security-Enhanced Linux (SELinux) firewall has been disabled. The firewall affects agent installation and should remain disabled until the agent is installed.

Installation Precautions


- For details about the OSs supported by the agent, see [Supported OSs](#).
- Ensure the outbound rule of your security group allows access to the port 10190 on the 100.125.0.0/16 network segment. (This is the default setting.)
- If any third-party security software has been installed on your server, the HSS agent may fail to be installed. In this case, disable or uninstall the software before installing the agent.

- The available capacity of the disk where the agent is installed must be greater than 300 MB. Otherwise, the agent installation may fail.
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Servers" tab of the "Asset Management > Servers & Quota" page.

Installing an Agent Using Commands

This procedure involves logging in to the server and running commands. It takes 3 to 5 minutes for the console to update the agent status after agent installation.

Step 1 Log in to the management console.

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

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

Step 4 Click the **Agents** tab. Click **Offline**. In the **Operation** column of a server, click **Install Agent**.

Step 5 In the displayed dialog box, copy the command suitable for your system architecture and OS.

Step 6 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, WinSCP, PuTTY, or Xshell, to log in to the server and install the agent on the server as user **root**.

Step 7 Paste the copied installation command and run it as user **root** 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 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 Windows

To enable workload protection for cloud servers, install the agent first.

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 Linux](#).

 **NOTE**

CentOS 6.x is no longer updated or maintained on the Linux official website, and HSS no longer supports CentOS 6.x or earlier.

Default Installation Path

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

C:\Program Files\HostGuard

Prerequisites


- Ensure the server runs Windows OS and can access the Internet.
- A remote management tool, such as mstsc and RDP, has been installed on your PC.

Installation Precautions

- For details about the OSs supported by the agent, see [Supported OSs](#).
- Ensure the outbound rule of your security group allows access to the port 10190 on the 100.125.0.0/16 network segment. (This is the default setting.)
- If any third-party security software has been installed on your server, the HSS agent may fail to be installed. In this case, disable or uninstall the software before installing the agent.
- The available capacity of the disk where the agent is installed must be greater than 300 MB. Otherwise, the agent installation may fail.
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Servers" tab of the "Asset Management > Servers & Quota" page.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Click the **Agents** tab. Click **Offline**. In the **Operation** column of a server, click **Install Agent**.

Step 5 In the displayed dialog box, copy the agent download link suitable for your system architecture and OS.

Step 6 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 mstsc or RDP, to log in to the server and install the agent on the server as an administrator.

Step 7 On the server where the agent is to be installed, use Internet Explorer to download the agent installation package from the copied agent download address and decompress it.

Step 8 Run the agent installation program as an administrator.

Step 9 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.

It takes 3 to 5 minutes for the console to update the agent status after agent installation.

----End

2.2 Enabling HSS

2.2.1 Enabling the Enterprise/Premium Edition

Before enabling protection on servers, you need to allocate quota to a specified server. If the protection is disabled or the server is deleted, the quota can be allocated to other servers.

For the WTP edition, choose **Prevention > Web Tamper Protection > Server Protection** and then enable it.

NOTE

To enable the WTP edition, choose **Prevention > Web Tamper Protection > Server Protection** and click the **Servers** tab. All the functions of the premium edition are included with the WTP edition.

Check Mode

HSS performs a full scan in the early morning every day.

After you enable server protection, you can view scan results after the automatic scan in the next early morning, or perform a manual scan.

Prerequisites

- The agent status of the server to be protected is **Online**. To check the status, choose **Asset Management > Servers & Quota** on the HSS.
- To better protect your containers, you are advised to set security configurations.


Restrictions

- 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, click , select a region, and choose **Security > Host Security Service**.

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

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

In the **Enable Protection** dialog box, select an HSS edition.

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

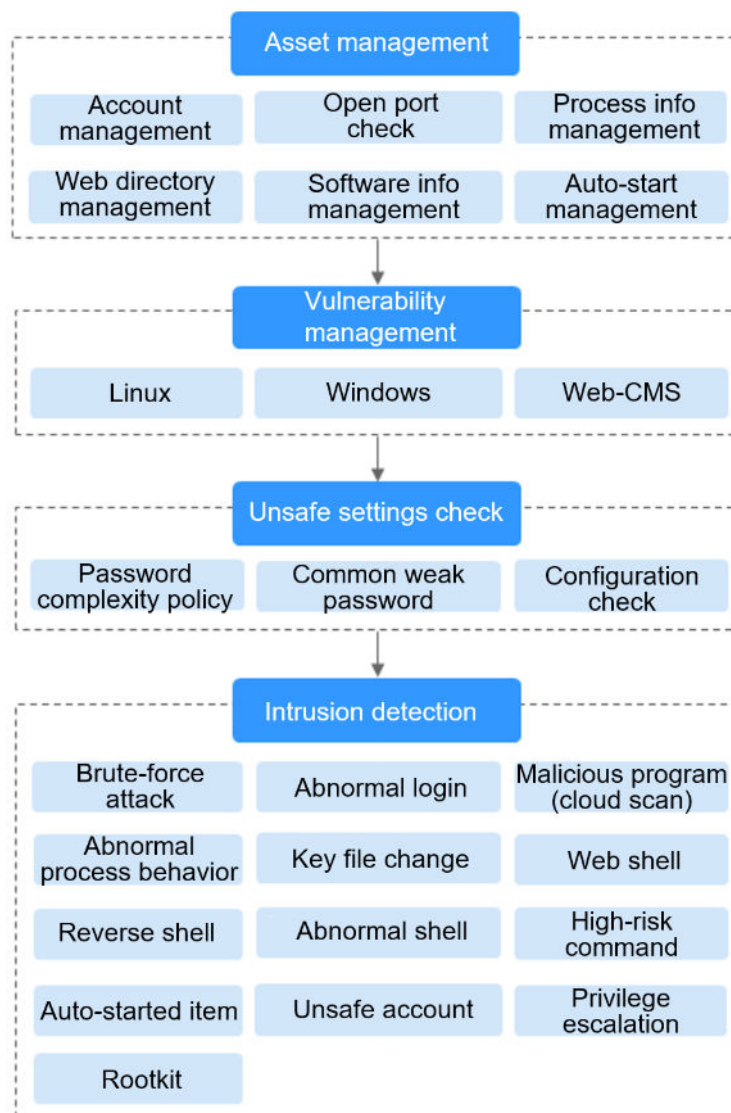
If the **Protection Status** of the target server is **Enabled**, the enterprise or premium edition has been enabled.

NOTE

- A quota can be bound to a server to protect it, on condition that the agent on the server is online.

After HSS is enabled, it will scan your servers for security issues. Check items vary according to the edition you enabled.

Figure 2-1 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.

On the left of the protection list, click **Risky**.

Click a server name to go to the details page. On this page, you can quickly check the detected information and risks of the server.

Follow-up Operation

You can manually configure check items. Configurable items vary according to the edition you enabled.

Figure 2-2 Manual check items

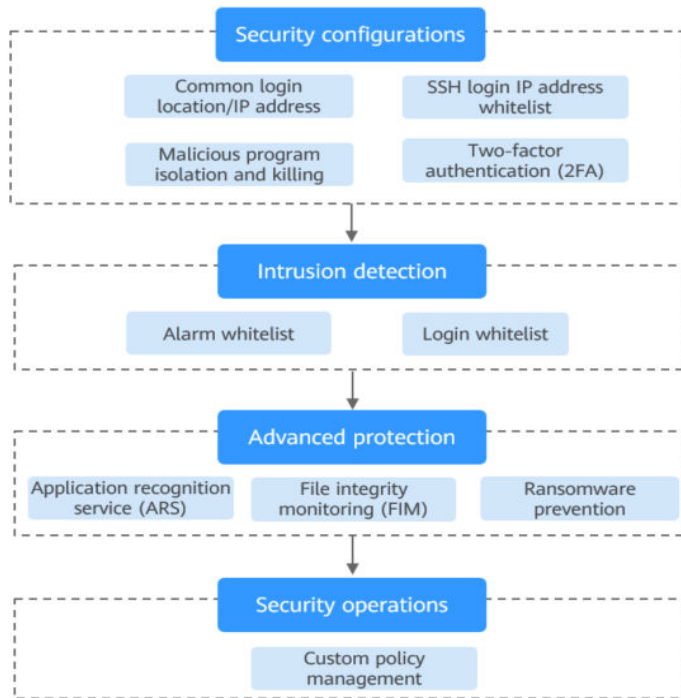


Table 2-1 Manual check items

Function	Check Item	Reference
Installation and configuration	<ul style="list-style-type: none"> Common login location/IP address SSH login IP address whitelist Isolate and kill malicious programs 	Installation and Configuration
Intrusion detection	<ul style="list-style-type: none"> Alarm whitelist Login whitelist 	Intrusion Detection
Proactive defense	<ul style="list-style-type: none"> Application protection File integrity monitoring (FIM) 	Prevention
Security operations	<ul style="list-style-type: none"> Policy management 	Security Operations
Security report	<ul style="list-style-type: none"> Subscribe to security reports 	Subscribing to a Security Report

Follow-Up Procedure

Disabling HSS

On the **Servers** tab of the **Servers & Quotas** 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.

2.2.2 Enabling the WTP Edition

Before enabling WTP, you need to allocate a quota to a specified server. If the service is disabled or the server is deleted, the quota can be allocated to other servers.

The premium edition will be enabled when you enable WTP.

How WTP Prevents Web Page Tampering

Table 2-2 Protection mechanisms

Type	Mechanism
Static web page protection	<ol style="list-style-type: none">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	<p>Provides runtime application self-protection (RASP) for Tomcat applications in the following ways:</p> <ol style="list-style-type: none">1. Malicious behavior filtering based on RASP The unique runtime application self-protection (RASP) detects application 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.

Prerequisites


- Choose **Prevention > Web Tamper Protection**. Click the **Servers** tab. The **Protection Status** of the server is **Unprotected**.
- Choose **Asset Management > Servers & Quota**. The **Agent Status** of a server is **Online**, and the **Protection Status** of the server is **Unprotected**.

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](#).
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.

Enabling WTP

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Prevention > Web Tamper Protection**. On the **Web Tamper Protection** page, click **Add Server**.
- Step 4** On the **Add Server** page, select the target server, select quota from the drop-down list or retain the default value, and click **Add and Enable Protection**.
- Step 5** View the server status on the **Web Tamper Protection** page.

The premium edition will be enabled when you enable WTP.

- Choose **Prevention > Web Tamper Protection**. If the **Protection Status** of the server is **Protected**, WTP has been enabled.
- Choose **Asset Management > Servers & Quota** and click the **Servers** tab. If the protection status of server is **Protected**, and **Disable** and **Switch Edition** are grayed out in the **Operation** column, the premium edition included with the WTP edition has been enabled.

----End

NOTICE

- A quota can be bound to a server to protect it, on condition that the agent on the server is online.
 - 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 **Prevention** > **Web Tamper Protection** and click the **Servers** tab. Click **Disable Protection** 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.
- The premium edition will be disabled when you disable WTP.

2.3 Enabling Container Node Protection

Before enabling protection for a container node, you need to allocate quota to a specified node. If the protection is disabled or the node is deleted, the quota can be allocated to other nodes.

Check Frequency

HSS performs a full check in the early morning every day.

If you enable server protection before the check interval, you can view check results only after the check at 00:00 of the next day is complete.


Constraints

Currently, HSS can only protect Docker containers.

Prerequisites

- The **Agent Status** of a server is **Online**. To check the status, choose **Asset Management** > **Containers & Quota**.
- You have created nodes on CCE.
- The **Protection Status** of the node is **Unprotected**.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Asset Management > Containers & Quota**.
- Step 4** In the **Operation** column of the node list, click **Enable Protection**.
- Step 5** In the displayed dialog box, confirm the server information.
- Step 6** Click **OK**. If the **Protection Status** of the server changes to **Protected**, protection has been enabled.

NOTE

A container security quota protects one cluster node.

----End

Follow-Up Procedure

Disabling protection for a node

Choose **Asset Management > Containers & Quota**, click the **Container Nodes** tab, and click **Nodes**. In the **Operation** column, click **Disable Protection**.

If protection is disabled, the quota status will change from occupied to idle. You can allocate the idle quota to another node to avoid quota waste.

NOTICE

- Before disabling protection, perform a comprehensive detection on the container, handle detected risks, and record operation information to prevent O&M errors and attacks on the container.
- After protection is disabled, clear important data on the container, stop important applications on the container, and disconnect the container from the external network to avoid unnecessary loss caused by attacks.

2.4 (Optional) Switching the HSS Edition

You can switch the quota edition of a server to the enterprise or premium edition as needed.

Precautions


You can switch to the enterprise or premium edition.

To use the WTP or container edition, apply for a quota of that edition and then enable it.

Prerequisites

- The server whose protection quota is to be changed is in the **Protected** state.
- Before switching to a lower edition, check the server, handle known risks, and record operation information to prevent O&M errors and attacks.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Asset Management > Servers & Quota**. Click the **Servers** tab.
- Step 4** In the **Operation** column of a server, click **Switch Edition**.

NOTICE

- If HSS 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 enterprise or premium edition. To use the WTP edition, you need to purchase and enable it separately.
-

- Step 5** Click **OK**.

The edition information in the **Edition** column will be updated. If the edition information in the **Edition** column is updated, the edition switch succeeded.

----End


Follow-up Procedure

- After the edition is switched, you can allocate the idle edition quota to other servers.
- After switching to a lower edition, clear important data on the server, stop important applications on the server, and disconnect the server from the external network to avoid unnecessary loss caused by attacks.
- After switching to a higher edition, perform a security detection on the server, handle security risks on the server, and configure necessary functions in a timely manner.

2.5 Installation and Configuration

After protection is enabled, you can configure the common login locations, common login IP addresses, and the SSH login IP address whitelist. You can also enable 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, click , select a region, 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 Choose **Installation & Configuration** and click the **Security Configuration** tab. Click **Common Login Locations** and click **Add Common Login Location**.

Step 2 In the dialog box that is displayed, select a geographical location and select servers. Confirm the information and click **OK**.

Step 3 Return to the **Security Configuration** tab of the **Installation & Configuration** page. Check whether the added locations are displayed on the **Common Login Locations** subtab.

----End

Configuring Common Login IP Addresses

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

Step 1 Choose **Installation & Configuration** and click the **Security Configuration** tab. Click **Common Login IP Addresses** and click **Add Common Login IP Address**.

Step 2 In the dialog box that is displayed, enter an IP address and select servers. Confirm the information and click **OK**.

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.
- Only one IP address can be added at a time. To add multiple IP addresses, repeat the operations until all IP addresses are added. Up to 20 IP addresses can be added.

Step 3 Return to the **Security Configuration** tab of the **Installation & Configuration** page. Check whether the added locations are displayed on the **Common Login IP Addresses** subtab.

----End

Configuring an SSH Login IP Address Whitelist

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

 NOTE

- An account can have up to 10 SSH login IP addresses in the whitelist.
- After you configure an SSH login IP address whitelist, SSH logins will be allowed only from whitelisted IP addresses.
 - Before enabling this function, ensure that all IP addresses that need to initiate SSH logins are added to the whitelist. Otherwise, you cannot remotely log in to your server using SSH.
If your service needs to access a server, but not necessarily via SSH, you do not need to add its IP address to the whitelist.
- Exercise caution when adding an IP address to the whitelist. This will make HSS no longer restrict access from this IP address to your servers.

Step 1 Choose **Installation & Configuration** and click the **Security Configuration** tab. Click **SSH IP Whitelist** and click **Add IP Address**.

Step 2 In the dialog box that is displayed, enter an IP address and select servers. Confirm the information and click **OK**.

 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.
- Only one IP address can be added at a time. To add multiple IP addresses, repeat the operations until all IP addresses are added.

Step 3 Return to the **Security Configuration** tab of the **Installation & Configuration** page. Check whether the added locations are displayed on the **Common Login IP Addresses** subtab.

----End

Isolating and Killing Malicious Programs

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

Programs are isolated and killed based on their confidence ratings. A high rating indicates a high probability that the detected program is a malicious program. To avoid mistakenly stopping trustworthy programs and affecting services, only the suspicious programs with a confidence rating of 95 or higher are automatically isolated and killed. You can manually isolate and kill programs with lower ratings. For details, see [Handling Server Alarms](#).

 NOTE

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

Step 1 Choose **Installation & Configuration** and click the **Security Configuration** tab. Click the **Isolation and Killing of Malicious Programs** tab and enable **Isolate and Kill Malicious Programs**.

 **NOTE**

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

Step 2 In the confirmation dialog box, click **OK** to enable the isolation and killing of 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 [Viewing Intrusion Alarms](#).

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**.

----End

Enabling 2FA

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

Prerequisites

- You have created a message topic whose protocol is SMS or email.
- Server protection has been enabled.
- To enable 2FA, you need to disable the SELinux firewall.

Constraints and Limitations

If 2FA is enabled, it can be used only in following scenarios:

- Linux: The SSH password is used to log in to an ECS, and the OpenSSH version is earlier than 8.
- Windows: The RDP file is used to log in to a Windows ECS.

Procedure

Step 1 On the **Two-Factor Authentication** tab, select servers and click **Enable 2FA**. Alternatively, click **Enable** in the **Operation** column.

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. For details, see "Creating a Topic" in *Simple Message Notification User Guide*.
- 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.

- **Verification code**

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

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

3 Server Security Dashboard

3.1 Risk Statistics

On the dashboard page of the HSS console, you can learn the security status and risks of all your servers and containers in real time, including the risk index, risk trend, top 5 event types, and service quota.

Step 1 Log in to the management console.

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

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

----End

Asset Risk Index (Last 7 Days)

You can check the risks in protected servers and containers in the last 7 Days.

To handle the risks, click **Handle Now**. The **Risks** pane will be displayed on the right. You can handle risks by referring to the corresponding guidance. You can handle the following types of risks:

- Intrusions
- Vulnerabilities
- Unsafe settings

To check your asset security, click **Scan**.

Protection Status (Last 24 Hours)

You can check the numbers of protected and unprotected servers and nodes.

To enable protection for a server, click **Enable Protection**.

Risks (Latest 24 Hours)

You can check the number of server asset risks, server vulnerabilities, server baselines, and container risks, and their comparison with the previous day.

Risk Statistics

You can check the risk trend in the last 24 hours, last 3 days, last 7 days, and last 30 days.

Table 3-1 Risk statistics

Category	Event
Asset risks	<ul style="list-style-type: none">• Accounts• Open ports• Processes• Installed software• Auto-started items• Web applications• Web services• Web frameworks• Websites• Middleware• Databases
Server vulnerabilities	<ul style="list-style-type: none">• Linux vulnerabilities• Windows vulnerabilities• Web-CMS vulnerabilities• Application vulnerabilities
Server baseline risks	<ul style="list-style-type: none">• Password complexity policy check• Common weak password check• Unsafe configuration check
Container risks	<ul style="list-style-type: none">• Local image vulnerabilities• Private image vulnerabilities• Malicious files in images• Image baseline

Intrusions (Last 24 Hours)

You can check the total number of intrusions detected on servers and containers, and the severities of the intrusions.

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

Top 5 Events

For servers protected by the enterprise, premium, or container security edition, you can check the top five types of intrusion events detected in the last 24 hours, last 3 days, last 7 days, or last 30 days; and the number of each type of events.

If no data is displayed due to connection problems, fix your network and click



to retrieve data again.

Real-time Alarms

You can check real-time alarms.

Check the latest five unhandled intrusion events in the last 24 hours, including their severities, alarm names, occurrence time, and statuses.

- To check alarm details, click an alarm name.
- To handle an alarm, click **Handle** in its **Operation** column. 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 24 hours.
- To check more alarm events, click **View More**.

4 Asset Management


4.1 Asset Management

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

Constraints

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

Procedure

- Step 1** Log in to the management console.
 - Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
 - Step 3** Choose **Asset Management > Assets**. Check your assets and their statistics.
- End


4.2 Server Fingerprints

4.2.1 Viewing Server Asset Fingerprints

HSS can collect server asset fingerprints, including information about ports, processes, web applications, web services, web frameworks, and auto-started items. You can centrally check server asset information and detect risky assets in a timely manner based on the server fingerprints. HSS does not touch your assets. You need to manually eliminate the risks.

Viewing Asset Information of All Servers

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

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

Step 3 Choose **Asset Management > Server Fingerprints** to view all server assets.

----End

Table 4-1 Asset fingerprints

Item	Description	Supported OS	Check Frequency
Accounts	<p>Check and manage all accounts on your servers to keep them secure.</p> <p>You can check real-time and historical account information to find suspicious accounts.</p> <ul style="list-style-type: none"> Real-time account information includes the account name, number of servers, server name/IP address, login permission, root permission, user group, user directory, shell started by the user, and the last scan time. Historical account change records include the server name/IP address, change status, login permission, root permission, user group, user directory, shell started by the user, and the last scan time. 	Linux and Windows	Real-time check
Open ports	<p>Check open ports on your servers, including risky and unknown ports.</p> <p>You can easily find high-risk ports by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files.</p> <ul style="list-style-type: none"> Manually disabling high-risk ports If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. For high-risk ports, check program files. If there are risks, delete or isolate the source files. It is recommended that you handle the ports at the Dangerous risk level promptly and handle the ports at the Unknown level based on the actual service conditions. Ignore risks: If a detected high-risk port is actually a normal port used for services, you can ignore it. The port will no longer be regarded risky or generate alarms. 	Linux and Windows	Real-time check

Item	Description	Supported OS	Check Frequency
Processes	<p>Check processes on your servers and find abnormal processes.</p> <p>You can easily identify abnormal processes based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes.</p> <p>If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.</p>	Linux and Windows	Real-time check
Installed software	<p>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.</p> <ul style="list-style-type: none"> • Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, and the last scan time. • Historical software change records include the server names, IP addresses, change statuses, software versions, software update time, and the last scan time. 	Linux and Windows	Automatic check every day
Auto-startup	<p>Check for auto-startup items and quickly locate Trojans.</p> <ul style="list-style-type: none"> • Real-time information about auto-started items includes their names, types (auto-started service, startup folder, pre-loaded dynamic library, Run registry key, or scheduled task), number of servers, server names, IP addresses, paths, file hashes, users, and the last scan time. • The historical change records of auto-started items include server names, IP addresses, change statuses, paths, file hashes, users, and the last scan time. 	Linux and Windows	Real-time check
Websites	<p>You can check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, certificate information (to be provided later), and key processes of websites.</p>	Linux	Once a week (06:00 a.m. every Monday)

Item	Description	Supported OS	Check Frequency
Web frameworks	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	Linux	Once a week (06:00 a.m. every Monday)
Middleware	You can check information about servers, versions, paths, and processes associated with middleware.	Linux and Windows	Once a week (06:00 a.m. every Monday)
Web services	You can check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software.	Linux	Once a week (06:00 a.m. every Monday)
Web applications	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software.	Linux and Windows (only Tomcat is supported)	Once a week (06:00 a.m. every Monday)
Databases	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software.	Linux and Windows (only MySQL is supported)	Once a week (06:00 a.m. every Monday)

Viewing Asset Information of a Single Server

- Step 1** Log in to the management console.
- Step 2** In the navigation pane, choose **Asset Management > Servers & Quota**. Click the **Servers** tab.
- Step 3** Click the name of the target server. On the server details page that is displayed, click the **Asset Fingerprints > Servers** tab.

Step 4 Click a fingerprint in the fingerprint list to view its asset information. For more information, see [Table 4-1](#).

----End

4.2.2 Viewing the Operation History of Server Assets

HSS proactively records the changes on account information, software information, and auto-started items. You can check the change details according to different dimensions and time ranges.

Checking Change Records

Step 1 Log in to the management console.

Step 2 Choose **Asset Management > Server Fingerprints** and click **Operation History**. On the displayed **Operation History** page, select a dimension and time period to view the change history of accounts, software, and auto-started items.

----End

Managing Account Information

Account changes are recorded.

- **Action:** 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).
- **Last Scan Time:** The last scan time indicates the time of the latest scan performed for servers in a period.

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.

Managing Software

Operations made to accounts are recorded.

- **Action: Create and Delete.**
- **Last Scan Time:** The last scan time records the time when the changes were detected, not the time 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.

Auto-started Items

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, IP addresses, changes, paths, file hashes, users, and last scan time of auto-startup items.

4.2.3 Manually Updating Server Asset Information in Real Time

This section describes how to obtain the latest information about web applications, web services, web frameworks, websites, middleware, and databases of your servers.

Constraints


- Only Linux servers are supported.
- The agent status of the server must be **Online**, and the agent version must be 3.2.5 or later. For details about how to check agent versions, see [Viewing Agent Management](#).

Check Frequency

Accounts and open ports are checked in real time. The open port detection result is updated every six hours.

Processes, web directories, software, and auto-startup items are automatically checked in the **early morning every day**.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Asset Management > Servers & Quota**. Click the **Servers** tab.
- Step 4** Click the name of the target server. On the server details page that is displayed, click the **Asset Fingerprints > Servers** tab.
- Step 5** Click a fingerprint type in the fingerprint list, and click **Discover Assets** on the upper area of the list on the right.

NOTE

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

- Step 6** After the automatic execution is complete, the last scan time is updated and the latest server asset information is displayed.

----End

4.3 Container Fingerprints

4.3.1 Viewing Container Asset Fingerprints


HSS can collect container asset fingerprints, including container clusters, services, workloads, accounts, ports, and processes. You can centrally check container asset information and detect risky assets in a timely manner based on the container fingerprints. This section describes how to view collected container asset information.

Constraints

- Only the HSS container edition supports the container fingerprint function.
- Only Linux is supported.

Viewing Asset Fingerprints Data of All Containers

Step 1 Log in to the management console.

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

Step 3 Choose **Asset Management** > **Container Fingerprints** > **Asset Fingerprints**. On the **Asset Fingerprints** page that is displayed, view the fingerprint data of all containers.

Table 4-2 Container asset fingerprints


Feature	Description	Check Frequency
Accounts	Check and manage all accounts on your containers to keep them secure. Real-time account information includes the account name, number of servers, server name, IP address, login permission, root permission, user group, user directory, shell started by the user, container name, container ID, and the last scan time.	Real-time check

Feature	Description	Check Frequency
Open ports	<p>Check open ports on your containers, including risky and unknown ports.</p> <p>You can easily find high-risk ports on containers by checking local ports, protocol types, server names, IP addresses, statuses, PIDs, and program files.</p> <ul style="list-style-type: none">Manually disabling high-risk ports If HSS detects open high-risk ports or unused ports, check whether they are really used by your services. For high-risk ports, check program files. If there are risks, delete or isolate the source files. <p>It is recommended that you handle the ports at the Dangerous risk level promptly and handle the ports at the Unknown level based on the actual service conditions.</p> <ul style="list-style-type: none">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.	Real-time check
Processes	<p>Check processes on your containers and find abnormal processes.</p> <p>You can easily identify abnormal processes on your containers based process paths, server names, IP addresses, startup parameters, startup time, users who run the processes, file permissions, PIDs, and file hashes.</p> <p>If a suspicious process has not been detected in the last 30 days, its information will be automatically deleted from the process list.</p>	Real-time check
Installed software	<p>Check and manage all software installed on your containers, and identify insecure versions.</p> <p>You can check real-time and historical software information to determine whether the software is risky.</p> <ul style="list-style-type: none">Real-time software information includes the software name, number of servers, server names, IP addresses, software versions, software update time, and the last scan time.Historical software change records include the server names, IP addresses, change statuses, software versions, software update time, and the last scan time.	Automatic check every day

Feature	Description	Check Frequency
Auto-started items	Check for auto-started items and quickly locate Trojans. Real-time information about auto-started items includes their names, types (auto-started service, startup folder, pre-loaded dynamic library, Run registry key, or scheduled task), number of servers, server names, IP addresses, paths, file hashes, users, container name, container ID, and the last scan time.	Real-time check
Website check	You can check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, certificate information (to be provided later), and key processes of websites.	Once a week (06:00 a.m. every Monday)
Web framework	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes.	Once a week (06:00 a.m. every Monday)
Middleware	You can also check information about servers, versions, paths, and processes associated with middleware.	Once a week (06:00 a.m. every Monday)
Web services	You can check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software.	Once a week (06:00 a.m. every Monday)
Web applications	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software.	Once a week (06:00 a.m. every Monday)
Database	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software.	Once a week (06:00 a.m. every Monday)

----End

Viewing Asset Fingerprint Data of a Single Container

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security** > Host Security Service.
- Step 3** In the navigation pane, choose **Asset Management** > **Servers & Quota**. Click the **Servers** tab.


Step 4 Click the name of the target server. On the server details page that is displayed, click the **Asset Fingerprints > Containers** tab.

Step 5 Click a fingerprint in the fingerprint list to view its asset information. For more information, see [Table 4-2](#).

----End

Viewing Cluster Information

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management > Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.


Step 6 On the **Clusters** page, view cluster information.

The **Clusters** page displays the cluster name, type, node, version, creation time, and status.

----End

Viewing Services

Step 1 Log in to the management console.

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


Step 3 In the navigation pane, choose **Asset Management > Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 6 On the **Services** tab page, view the information.


The page displays the service name, endpoint name, access mode, service IP address, namespace, cluster, and creation time.

- Searching for a service
You can enter information such as the service name and access mode in the search box and click  to search for the service.
- Viewing details about a service
Click the name of a service. On the service details page that is displayed, you can view the selector, tag, and port of the service.

----End

Viewing Endpoints

Step 1 Log in to the management console.

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


Step 3 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 6 Choose **Services** > **Endpoints**. View endpoints information.


The page displays the endpoint name, namespace, cluster, associated with service, service name, and creation time.

- Searching for an endpoint
You can enter information such as the endpoint name and namespace in the search box and click  to search for the endpoint.
- Viewing details about an endpoint
Click the name of an endpoint. On the endpoint details page that is displayed, you can view the pod mapping and port information.

----End

Viewing a Workload

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 6 Click the **Workloads** tab.

Step 7 Select different workloads and view information.

You can view information about **Deployment**, **StatefulSets**, **DaemonSets**, **Jobs**, **Cron Jobs**, and **Pods**. For details about the information items, see [Workload information Items](#).


You can enter information such as the workload name and cluster in the search box and click  to search for the target workload.

Table 4-3 Workload information


Workload Type	Item
Deployment	<ul style="list-style-type: none">• Workload name• Status• Instances• Namespaces• Created• Image name• Cluster
StatefulSets	<ul style="list-style-type: none">• Workload name• Status• Instances• Namespace• Created• Image name• Cluster
DaemonSets	<ul style="list-style-type: none">• Workload name• Status• Instances• Namespace• Created• Image name• Cluster
Jobs	<ul style="list-style-type: none">• Workload name• Status• Instances• Namespace• Created• Image name• Cluster

Workload Type	Item
Cron Jobs	<ul style="list-style-type: none"> • Workload name • Status • Trigger • Running jobs • Namespace • Latest scheduled • Created • Image name • Cluster
Pods	<ul style="list-style-type: none"> • Name • Namespace • Cluster • Node • Pod IP address • POD IP • Status • Created

----End

Viewing Container Instances

Step 1 Log in to the management console.

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


Step 3 In the navigation pane, choose **Asset Management** > **Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

Step 6 Click the **Container Instances** tab.

The container name, status, pod, cluster, creation time, and image name are displayed.

- Searching for a container
You can enter information such as the container name and status in the search box and click  to search for the container.
- Viewing details about a container

Click the name of a container. On the container details page that is displayed, you can view the process, port, and mount path.

----End

4.3.2 Manually Updating Container Asset Information in Real Time


This section describes how to obtain the latest asset fingerprints, clusters, services, workloads, and containers.

Constraints

- Only the HSS container edition supports the container fingerprint function.
- Only Linux is supported.
- The agent status of the server must be **Online**, and the agent version must be 3.2.5 or later. For details about how to check agent versions, see [Viewing Agent Management](#).

Updating Container Fingerprint Data in Real Time

Step 1 Log in to the management console.

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

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

Step 4 Click the name of the target server. On the server details page that is displayed, click the **Asset Fingerprints > Containers** tab.

Step 5 Click a fingerprint type in the fingerprint list, and click **Discover Assets** on the upper area of the list on the right.

NOTE


Currently, only **Web applications**, **Web services**, **Web frameworks**, **Websites**, **Middleware**, and **Databases** support real-time manual collection and update. Information about other types is automatically collected and updated every day.

Step 6 After the automatic execution is complete, the last scan time is updated and the latest container asset information is displayed.

----End

Updating Information About Clusters, Services, Workloads, and Containers In Real Time

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management > Container Fingerprints**.

Step 4 Choose **Clusters** and click **Synchronize** in the upper left corner.

Step 5 **Last Synchronized** indicates the CCE cluster, service, workload, and container data is synchronized successfully.

----End


4.4 Server Management

4.4.1 Viewing Server Protection Status


The server list on the **Servers** page displays the protection status of only the servers used in the selected region.

Viewing the Server List

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management** > **Servers & Quota**. On the **Servers** tab, view the protection status of the server. For more information, see [Table 4-4](#).

You can check the server name, ID, IP address, OS, running status. To set the items to be displayed in the server protection list, click  in the upper right corner.


- To check the protection status of a server, enter a server name, server ID, or IP address in the search box above the server protection list, and click .
- On the left of the server protection list, select a server protection edition or an asset importance category to view the protection status of each type of servers.

Table 4-4 Protection status description

Parameter	Description
Agent Status	<ul style="list-style-type: none">• 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.

Parameter	Description
Action	<ul style="list-style-type: none"> • Enabled: The server is fully protected by HSS. • Unprotected: HSS is disabled for the server. Click Enable in the Operation column to enable HSS for the server. • Protection interrupted: The server is shut down, the agent communication is abnormal, or the agent is uninstalled.
Scan Results	<ul style="list-style-type: none"> • Risky: The host has risks. • Safe: No risks are found. • Pending risk detection: HSS is not enabled for the server.

----End

Viewing the WTP Status

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Prevention > Web Tamper Protection** and click **Servers** to view the protection status of the servers.




To check the protection status of a target server, enter a server name, server ID, or IP address in the search box above the protection list, and click .

Table 4-5 Statuses


Parameter	Description
Protection Status	Protected: HSS provides static web tamper protection (WTP) for the server.
Dynamic WTP	Status of dynamic WTP, which can be: <ul style="list-style-type: none"> •  : Enabling dynamic WTP •  : Disabling dynamic WTP (After enabling dynamic WTP, restart Tomcat to make this setting take effect.)
Static Tampering Attacks	Number of times that static web page files are attacked and tampered with.
Dynamic Tampering Attacks	Number of web application vulnerability exploits and injection attacks.

----End

Exporting the Server List

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Asset Management > Servers & Quota**. The **Servers** tab page is displayed.

Step 3 Click  in the upper right corner of the **Server** tab page to export the details of the server list.

 **NOTE**

The details of up to 1000 servers can be exported at a time.

----End

4.4.2 Enabling Protection

4.4.2.1 Enterprise/Premium Edition

The enterprise and premium editions provides different levels of protection for your servers. You can apply for and enable them as needed.

Check Frequency

HSS performs a full scan in the early morning every day.

After you enable server protection, you can view scan results after the automatic scan in the next early morning, or perform a manual scan immediately.

Prerequisite


The agent has been installed on the servers to be protected, the agent status is **Online**, and the protection status is **Unprotected**.

Constraints

- Linux
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
 - 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.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Enable protection for one or multiple servers.

- **Enabling protection for a server**

Click **Enable** in the **Operation** column of a server. In the dialog box that is displayed, confirm the server information.

Table 4-6 Protection parameters

Parameter	Description	Example Value
Edition	<p>Select the enterprise or premium edition.</p> <ul style="list-style-type: none"> - Enterprise edition: It provides support for the DJCP MLPS certification. Main features include asset fingerprint management, vulnerability management, malicious program detection, web shell detection, and abnormal process behavior detection. - Premium edition: It helps you with the DJCP MLPS certification and provides advanced features, including application protection, ransomware prevention, high-risk command detection, privilege escalation detection, and abnormal shell detection. 	Enterprise

- **Enabling protection in batches**

Select multiple servers and click **Enable** above the server list. In the dialog box that is displayed, confirm the server information.

Table 4-7 Protection parameters

Parameter	Description	Example Value
Edition	<p>Select the enterprise or premium edition.</p> <ul style="list-style-type: none"> - Enterprise edition: It provides support for the DJCP MLPS certification. Main features include asset fingerprint management, vulnerability management, malicious program detection, web shell detection, and abnormal process behavior detection. - Premium edition: It helps you with the DJCP MLPS certification and provides advanced features, including application protection, ransomware prevention, high-risk command detection, privilege escalation detection, and abnormal shell detection. 	Enterprise

Step 5 Confirm the information and click **OK**. If the protection status of the target servers is **Protected**, the protection has been enabled.

----End

4.4.2.2 WTP Edition

The WTP edition provides web tamper protection capabilities for your servers.

How WTP Prevents Web Page Tampering

Table 4-8 How WTP works

Type	Mechanism
Static web page protection	<ol style="list-style-type: none">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. Proactive 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 server to restore the file.3. Remote backup and restoration If a file directory or backup directory on the local server is invalid, you can use the remote backup service to restore the tampered web page.
Dynamic web page protection	<p>Dynamic web page protection for Tomcat.</p> <ol style="list-style-type: none">1. Malicious behavior filtering based on RASP The unique runtime application self-protection (RASP) detects application 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.

Prerequisite


- The agent has been installed on the servers to be protected, the agent status is **Online**, and the protection status is **Unprotected**.

Configuring Protected Directories

You can add up to 50 directories to be protected. For details, see [Adding a Protected Directory](#).

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.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Protection > Web Tamper Protection**. On the **Web Tamper Protection** page, click the **Servers** tab.
- Step 4** Click **Add Server**. In the displayed dialog box, select servers.

 **NOTE**

Selected servers must be equal to or fewer than the available quotas.

- Step 5** Click **Add and Enable Protection** and check the protection status. Choose **Protection > Web Tamper Protection**. On the **Web Tamper Protection** page, click the **Servers** tab. If the **Protection Status** of the server is **Protected**, WTP has been enabled.

NOTICE

- After WTP is enabled, configure protected directories for WTP to take effect. For details, see [Adding a Protected Directory](#).
- Dynamic WTP can only be enabled for Linux servers, and can only be used after Tomcat is restarted.
- You can check the server protection status on the **Web Tamper Protection** page.

The premium edition will be enabled when you enable WTP. You can perform the following operations to check the protection status:

- Choose **Prevention > Web Tamper Protection**. If the **Protection Status** of the server is **Protected**, WTP has been enabled.
- Choose **Asset Management > Servers & Quota** and click the **Servers** tab. If the protection status of server is **Protected**, and **Disable** and **Switch Edition** are grayed out in the **Operation** column, the premium edition included with the WTP edition has been enabled.

----End

4.4.3 Disabling Protection


4.4.3.1 Enterprise/Premium Edition

You can disable protection for a server. A quota that has been unbound from a server can be bound to another one.

Precautions

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

Disabling Protection

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Asset Management > Servers & Quota**. Click the **Servers** tab.
- Step 4** Disable protection for one or multiple servers.
- **Disabling protection for a server**
 - a. Click **Disable** in the **Operation** column of a server.
 - b. In the dialog box that is displayed, confirm the information and click **OK**.
 - c. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

 **CAUTION**

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

- **Disabling protection in batches**
 - a. Select multiple servers and click **Disable** above the server list.
 - b. In the dialog box that is displayed, confirm the information and click **OK**.
 - c. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

 **CAUTION**

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

----End

4.4.3.2 WTP Edition


You can disable the WTP edition for a server. A quota that has been unbound from a server can be bound to another one.

Precautions

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

Procedure

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

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

Step 3 In the navigation pane, choose **Protection > Web Tamper Protection**. On the **Web Tamper Protection** page, click the **Servers** tab.

Step 4 Click **Disable** in the **Operation** column.

 **NOTE**

The WTP edition cannot be disabled for servers in batches.

Step 5 In the dialog box that is displayed, confirm the information and click **OK**.

Step 6 Choose **Asset Management > Servers & Quota** and click the **Servers** tab. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

 **CAUTION**

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

----End

4.4.4 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 policy group of this edition (including weak password and website shell detection policies) takes effect for all your servers by default.
- When you enable the premium edition alone or the premium edition included with the WTP edition, the policy group of this edition takes effect by default.
To create your own policy group, you can copy the policy group of premium edition and add or remove policies in the copy.

Creating a Policy Group

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Security Operations > Policies**

Step 4 Copy a policy group.

- Select the **tenant_linux_premium_default_policy_group** policy group. Locate the row that this policy group resides, click **Copy** in the **Operation** column.

- Select the **tenant_windows_premium_default_policy_group** policy group. Click **Copy** in the **Operation** column.

Step 5 In the dialog box displayed, enter a policy group name and description, and click **OK**.


 **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.

Step 6 Click **OK**.

Step 7 Click the name of the policy group you just created. The policies in the group will be displayed.

Step 8 Click a policy name and modify its settings as required. For details, see [Modifying a Policy](#).

Step 9 Enable or disable the policy by clicking the corresponding button in the **Operation** column. You can click  to refresh the page.

----End

Applying a Policy Group

Step 1 Log in to the HSS management console.

Step 2 In the navigation pane, choose **Asset Management > Servers & Quota** and click **Servers**.

Step 3 On the **Devices** page, select one or more target hosts and click **Apply Policy**.

Step 4 In the dialog box that is displayed, select a policy group and click **OK**.

 **NOTE**

- Old policies applied to a server will become invalid if you apply new policies to the server.
- Policies are applied to the servers within 1 minute.
- Policies applied to offline servers will not take effect until the servers are online.
- In a deployed policy group, you can enable, disable, or modify policies.
- A policy group that has been deployed cannot be deleted.

----End

4.4.5 Managing Server Groups


To manage servers by group, you can create a server group and add servers to it.

You can check the numbers of servers, unsafe servers, and unprotected servers in a group.

Creating a Server Group

After creating a server group, you can add servers to the group for unified management.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Asset Management > Servers & Quota**, click **Server Groups** in the **Server** list, and click **Create Server Group**.

Step 4 In the **Create Server Group** dialog box, enter a server group name and select the servers to be added to the group.

NOTE

- A server group name must be unique, or the group will fail to be created.
- A name cannot contain spaces. It contains only letters, digits, underscores (_), hyphens (-), dots (.), asterisks (*), and plus signs (+). The length cannot exceed 64 characters.

Step 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**.

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 Click **Servers & Quota** and click **Server Groups** on the **Servers** tab.

Step 2 Locate the row where a server group resides and click **Edit** in the **Operation** column.

Step 3 In the displayed dialog box, change the server group name and add or remove servers in the group.

Step 4 Click **OK**.

----End

Deleting a server group

Step 1 Click **Servers & Quota** and click **Server Groups** on the **Servers** tab.

Step 2 Locate the row where a server group resides and click **Delete** in the **Operation** column.

NOTE

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

----End

4.4.6 Configuring Asset Importance


By default, HSS considers all servers as general assets. You can configure the asset importance levels of servers and manage servers accordingly.

Assets are classified into the following types:

- **Important.** Specify this level for servers that run important services or store important data.
- **General.** Specify this level for servers that run general services or store general data.
- **Test.** Specify this level for servers that run test services or store test data.

Checking Asset Importance

Step 1 Log in to the management console.

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

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

Step 4 In the lower part of the tab page, check the asset importance. You can click **Important**, **General**, or **Test** to view servers by importance level.

----End

Specifying Asset Importance

Step 1 Log in to the HSS management console.

Step 2 In the navigation pane, choose **Asset Management > Servers & Quota**. Click the **Servers** tab.

Step 3 Configure asset importance.

- Configuring a server
 - Method 1: Select a server and configure its asset importance.

- i. Select a server and click **Configure Asset Importance**.
 - ii. In the dialog box that is displayed, select an asset importance level.
 - iii. Confirm the information and click **OK**.
- Method 2: Click the configuration button in the **Operation** column.
- i. In the **Operation** column of a server, choose **More > Configure Asset Importance**.
 - ii. In the dialog box that is displayed, select an asset importance level.
 - iii. Confirm the information and click **OK**.
- Configuring servers in batches
 - a. Select multiple servers and click **Configure Asset Importance**.
 - b. In the dialog box that is displayed, select an asset importance level.
 - c. Confirm the information and click **OK**.

----End

4.5 Container Management

4.5.1 Viewing the Clusters and Protection Quotas


The **Container Nodes** page displays the protection, node, and agent status of clusters, helping you learn the security status of clusters in real time.

Constraints

- Only Linux servers are supported.
- Servers that are not protected by HSS enterprise, premium, WTP, or container editions cannot perform container-related operations.

Checking the Node List

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Asset Management > Containers & Quota**. Click **Container Nodes**.

Step 4 View the node protection status on the **Nodes** page. You can obtain the details in [Table 4-9](#).

NOTE

In the HSS container node list, you can view only the servers where the agent has been installed. To view the servers where the agent has not been installed, choose **Asset Management > Servers & Quota**.

Table 4-9 Parameter description

Parameter	Description
Server Name	Target server name
Protection Status	Protection status of a node. The options are as follows: <ul style="list-style-type: none">• Unprotected• Protected• Protection interrupted
Server Status	<ul style="list-style-type: none">• Running• Unavailable• Normal
Agent Status	You can select a status to view the server. <ul style="list-style-type: none">• Online• Offline• Not installed

----End

4.5.2 Enabling Container Security Protection

You can enable the container security edition for your containers.

To enable protection for a container node, you need to allocate a quota to the node. If the protection is disabled or the node is deleted, the quota can be allocated to another node.

Check Frequency

HSS performs a full check in the early morning every day.

After you enable server protection, you can view scan results after the automatic scan in the next early morning.

Constraints


Currently, HSS can only protect Docker containers.

Prerequisite

- The **Agent Status** of a server is **Online**. To check the status, choose **Host Security Service > Asset Management > Containers & Quota**.
- You have created a node on CCE.
- The **Protection Status** of the node is **Unprotected**.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Enable protection for one or multiple servers.

- **Enabling protection for a server**

- a. In the **Operation** column of a server, click **Enable Protection**.
- b. In the dialog box that is displayed, confirm the information.

 **NOTE**

A container security quota protects one cluster node.

- c. Confirm the information and click **OK**. If the **Protection Status** in the container list changes to **Protected**, it indicates the protection has been enabled.

- **Enabling protection in batches**

- a. In the node list, select servers, and click **Enable Protection** above the list.
- b. In the dialog box that is displayed, confirm the information.

 **NOTE**

A container security quota protects one cluster node.

- c. Confirm the information and click **OK**. If the **Protection Status** in the container list changes to **Protected**, it indicates the protection has been enabled.

----End

4.5.3 Disabling Container Security Protection


You can disable the container edition for a server. A quota that has been unbound from a server can be bound to another one.

Before You Start

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Disable protection for one or multiple servers.

- **Disabling protection for a server**
 - a. In the node list, click **Disable Protection** in the **Operation** column of a server.
 - b. In the dialog box that is displayed, confirm the information and click **OK**.
 - c. Choose **Asset Management > Containers & Quota** and click the **Container Nodes** tab. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

CAUTION

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

- **Disabling protection in batches**
 - a. In the node list, select servers, and click **Disable Protection** above the list.
 - b. In the dialog box that is displayed, confirm the information and click **OK**.
 - c. Choose **Asset Management > Containers & Quota** and click the **Container Nodes** tab. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

CAUTION

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

----End

4.5.4 Container Images

4.5.4.1 Local Images


You can manually scan local images for vulnerabilities and software information and provides scan reports. This section describes how to perform security scans on local images and view scan reports.

Constraints

- Only the HSS container edition supports this function.
- Only the local images of the Docker engine can be reported to the HSS console.
- Security scans can be performed only on Linux images.

Viewing Local Images

Step 1 Log in to the management console.

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

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

Step 4 Click the **Container Images** tab and click **Local image**.

You can view the name, version, type, and security risks of an image.

- Viewing information about servers associated with an image
Locate the row that contains the target image and click the number in the **Associated Servers** column. The **Associated Servers** page is displayed. You can view details about the servers associated with the image.
- Viewing information about containers associated with an image
Locate the row that contains the target image and click the number in the **Associated Containers** column. The **Associated Containers** page is displayed. You can view details about the containers associated with the image.
- Viewing information about image components
Locate the row that contains the target image and click the number in the **Components** column. The **Components** page is displayed. You can view details about image components.

----End

Local Image Security Scans

The security scan items are as follows:

Scan Item	Description
Vulnerability	Detects vulnerabilities in images.
Installed software	Collects software information in an image.

Step 1 Log in to the HSS management console.

Step 2 In the navigation pane, choose **Asset Management > Containers & Quota**.

Step 3 Click the **Container Images** tab and click **Local image**.

Step 4 Performs a security scan for a single image or multiple images.

- Single image security scan
In the **Operation** column of the target image, click **Scan** to perform security scan.
- Batch image security scan
Select all target images and click **Scan** above the image list to perform security scan for multiple target images.
- Full image security scan
Click **Scan All** above the image list to perform a security scan for all images.

- Step 5** The image security scan is complete, when the **Scan Status** changes to **Completed** and the **Latest Scan Completed** shows the latest task execution time.
- End

Viewing Local Image Vulnerability Reports and Software Information

- Step 1** Log in to the HSS management console.
- Step 2** In the navigation pane on the left, choose **Asset Management > Containers & Quota**. Click the **Container Images** tab and click **Local image** to view the image scan result.
- End

Exporting Local Image Vulnerability Reports

- Step 1** Log in to the HSS management console.
- Step 2** In the navigation pane, choose **Asset Management > Containers & Quota**.
- Step 3** Click the **Container Images** tab and click **Local image**.
- Step 4** Click **Export Vulnerability** above the image list.

If you want to export the vulnerability report of a specified image, select the image type in the search box and click **Export Vulnerability**.

----End


4.5.5 Viewing Container Information

You can view container information on the **Containers** page to learn about the container status, cluster, and risks. This section describes how to view container information.

Constraints

- Only the HSS container edition supports this function.
- Only the local images of the Docker engine can be reported to the HSS console.
- Security scans can be performed only on Linux images.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Asset Management > Containers & Quota**.
- Step 4** Choose **Containers**. The container page is displayed.
- Step 5** View the container information and security status.

In the container list, you can view the container name, status, risks, restart times, POD, and cluster.

- View container details.

Click the name of the target container. On the container details page that is displayed, view the container image, process, port, and mount path information.

- View the container risk distribution.

View the number of low-risk, medium-risk, high-risk, and critical risks in the container.

----End

4.5.6 Handling Risk Containers

Scenario

HSS can detect container security risks and classify them into the following types:

- Critical: malicious program
- High risk: ransomware attacks, malicious programs, reverse shells, escape attacks, and dangerous commands
- Medium risk: web shell, abnormal startup, process exception, and sensitive file access
- Low risk: brute-force attack


To prevent containers with medium or higher security risks from affecting other containers, you can isolate, suspend, or kill risky containers.

Constraints

- Only the HSS container edition supports this function.
- Only Linux containers are supported.
- Only containers with medium or higher security risks can be handled.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Choose **Containers**. The container page is displayed.

Step 5 Enter **Risk** in the search box and click  to filter containers with security risks.

Step 6 In the **Operation** column of the target risky container, select the operation to be performed.

Cluster containers can be killed. Single-node containers can be isolated, suspended, and killed.

 **NOTE**

Only containers with medium or higher risks can be handled. You can view the security risk distribution.

- **Isolate containers:** After a container is isolated, you cannot access the container when the container is running, and the container cannot access the mount directory of the host or the system file of the container.
 - a. Click **Isolate**.
 - b. In the dialog box that is displayed, click **OK**.
- **Suspend containers:** Freeze the processes running in the container.
 - a. Click **Suspend**.
 - b. In the dialog box that is displayed, click **OK**.
- **Kill containers:** Terminate a running container process. If **autoremove** is configured for the container, the container cannot be resumed.
 - a. Click **Kill** to kill the container.
 - b. In the dialog box that is displayed, click **OK**.

----End

Follow-up Procedure

Restoring a container to the running state

Restores a container from the **Isolate**, **Waiting**, or **Terminated** state to the **Running** state.

 **NOTE**

If **autoremove** is configured for a terminated container, the container cannot be resumed.

Step 1 In the row containing the target container, click **Restore** in the **Operation** column.

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

----End

5 Risk Prevention

5.1 Vulnerability Management

5.1.1 Vulnerability Management Overview

Vulnerability management can detect Linux, Windows, Web-CMS, and application vulnerabilities and provide suggestions, helping you learn about server vulnerabilities in real time. Linux and Windows vulnerabilities can be fixed in one-click mode. This section describes how the vulnerabilities are detected and the vulnerabilities that can be scanned and fixed in each HSS edition.

 **NOTE**

The vulnerability list displays vulnerabilities detected in the last seven days. After a vulnerability is detected for a server, if you change the server name and do not perform a vulnerability scan again, the vulnerability list still displays the original server name.

How Vulnerability Scan Works

[Table 5-1](#) describes how different types of vulnerabilities are detected.

Table 5-1 How vulnerability scan works

Type	Mechanism
Linux vulnerability	Based on the vulnerability database, checks and handles vulnerabilities in the software (such as kernel, OpenSSL, vim, glibc) you obtained from official Linux sources and have not compiled, reports the results to the management console, and generates alarms.
Windows vulnerability	Synchronizes Microsoft official patches, checks whether the patches on the server have been updated, pushes Microsoft official patches, reports the results to the management console, and generates vulnerability alarms.

Type	Mechanism
Web-CMS vulnerability	Checks web directories and files for Web-CMS vulnerabilities, reports the results to the management console, and generates vulnerability alarms.
Application vulnerability	Detects the vulnerabilities in the software and dependency packages running on the server, reports risky vulnerabilities to the console, and displays vulnerability alarms.

Types of Vulnerabilities That Can Be Scanned and Fixed

For details about the types of vulnerabilities that can be scanned and fixed in different HSS editions, see [Table 5-2](#).

The meanings of the symbols in the table are as follows:

- √: supported
- ×: not supported

Table 5-2 Types of vulnerabilities that can be scanned and fixed in each HSS edition

Vulnerability Type	Function	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
Linux vulnerability	Automatic vulnerability scan (once a week by default)	√	√	√	√
	Vulnerability policy configuration	√	√	√	√
	Manual vulnerability scan	√	√	√	√
	One-click vulnerability fix	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√	√	√

Vulnerability Type	Function	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
Windows vulnerability	Automatic vulnerability scan (once a week by default)	√	√	√	×
	Vulnerability policy configuration	√	√	√	×
	Manual vulnerability scan	√	√	√	×
	One-click vulnerability fix	√ (A maximum of 50 vulnerabilities can be fixed at a time.)	√	√	×
Web-CMS vulnerability	Automatic vulnerability scan (once a week by default)	√	√	√	√
	Vulnerability policy configuration	√	√	√	√
	Manual vulnerability scan	√	√	√	√
	One-click vulnerability fix	×	×	×	×
Application vulnerability	Automatic vulnerability scan (once a week by default)	√	√	√	√
	Vulnerability policy configuration	√	√	√	√
	Manual vulnerability scan	√	√	√	√

Vulnerability Type	Function	Enterprise Edition	Premium Edition	Web Tamper Protection Edition	Container Edition
	One-click vulnerability fix	×	×	×	×

NOTE

- HSS can scan for Web-CMS and application vulnerabilities but cannot fix them. You can log in to your server to manually fix the vulnerability by referring to the suggestions displayed on the vulnerability details page.
- You can configure the automatic scan period, automatic scan scope, and vulnerability whitelist. For details about how to configure the automatic scan period and automatic scan scope, see [Automatic Vulnerability Scan](#). For details about how to configure the vulnerability whitelist, see [Managing the Vulnerability Whitelist](#).

5.1.2 Vulnerability Scan

To view real-time vulnerabilities of a server, you can manually scan for vulnerabilities.


HSS can scan for Linux, Windows, Web-CMS, and application vulnerabilities. Automatic and manual scans are supported.

- Automatic scan: You can configure the scan period and scope to periodically scan for vulnerabilities on servers.
- Manual scan: To view real-time vulnerabilities of a server, you can manually scan for vulnerabilities.

This section describes how to set an automatic scan policy and manually scan for vulnerabilities.

Manual Vulnerability Scan

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction > Vulnerabilities**.

Step 4 Click **Scan** in the upper right corner of the **Vulnerabilities** page.

Step 5 In the **Scan for Vulnerability** dialog box displayed, select the vulnerability type and scope to be scanned. For more information, see [Table 5-3](#).

Table 5-3 Parameters for manual scan vulnerabilities

Parameter	Description
Type	Select one or more types of vulnerabilities to be scanned. Possible values are as follows: <ul style="list-style-type: none">• Linux• Windows• Web-CMS• Application
Scan	Select the servers to be scanned. Possible values are as follows: <ul style="list-style-type: none">• All servers• Selected servers You can select a server group or search for the target server by server name, ID, EIP, or private IP address. NOTE The following servers cannot be selected for vulnerability scan: <ul style="list-style-type: none">• Servers that are not in the Running state• Servers whose agent status is Offline

Step 6 Click **OK**.

Step 7 Click **Manage Task** in the upper right corner of the **Vulnerabilities** page. On the **Manage Task** slide-out panel displayed, click the **Scan Tasks** tab to view the status and scan result of the vulnerability scan task.

Click the number next to the red figure in the **Scan Result** column to view information about the servers that fail to be scanned.

 **NOTE**


You can also choose **Asset Management > Servers & Quota** and scan a single server for vulnerabilities on the **Servers** tab. The procedure is as follows:

1. Click a server name.
2. Choose **Vulnerabilities**.
3. Choose the vulnerability type to be scanned and click **Scan**.

----End


Automatic Vulnerability Scan

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction > Vulnerabilities**.

Step 4 In the upper right corner of the **Vulnerabilities** page, click **Configure Policy** to set the vulnerability scan period and scope.

- **Scan Period**
 - **Scan period:** The default value is **00:00:00 - 07:00:00** and cannot be changed.
 - **Scan Period:** Select **Every day**, **Every three days**, or **Every week**.
- **Scan**
 - Enable or disable server scan:  indicates that server scan is enabled.
 - Select the servers to scan: Click **Select Server to Scan**. On the server management page displayed, select the servers to be scanned.

NOTE

The following servers cannot be selected for vulnerability scan:

- Servers that are not in the **Running** state
- Servers whose agent status is **Offline**

Step 5 Click **Manage Task** in the upper right corner of the **Vulnerabilities** page. On the **Manage Task** slide-out panel displayed, click the **Scan Tasks** tab to view the status and scan result of the vulnerability scan task.

Click the number next to the red figure in the **Scan Result** column to view information about the servers that fail to be scanned.

----End

5.1.3 Viewing Vulnerability Details


You can view vulnerabilities of your assets on the **Vulnerabilities** page.

Constraints

- Servers that are not protected by HSS do not support this function.
- The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**. Otherwise, vulnerability scan cannot be performed.

Viewing Vulnerability Details

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction > Vulnerabilities**.




Step 4 View vulnerability information on the **Vulnerabilities** page.

- Viewing vulnerability scan results

In the vulnerability statistics area in the upper part of the **Vulnerabilities** page, view vulnerability scan results. [Table 5-4](#) describes related parameters.

Table 5-4 Vulnerability scan parameters

Parameter	Description
Critical Vulnerabilities	Click the number in Critical vulnerabilities . On the slide-out panel displayed, you can view all types of vulnerabilities to be urgently fixed.
Unfixed Vulnerabilities	Click the number in Unfixed Vulnerabilities . On the slide-out panel displayed, you can view all types of vulnerabilities that are not fixed.
Servers with Vulnerabilities	Click the number in Servers with Vulnerabilities . You can view the servers with vulnerabilities in the lower part of the Vulnerabilities page.
Vulnerabilities Handled Today	Click the number in Vulnerabilities Handled Today . On the slide-out panel displayed, you can view all types of vulnerabilities that have been handled today.
Vulnerabilities Handled in Total	Click the number in Vulnerabilities Handled in Total . On the slide-out panel displayed, you can view all types of vulnerabilities that have been handled. The number is just the quantity of vulnerabilities handled within one year.
Detectable Vulnerabilities	Displays the number of vulnerabilities that can be detected by HSS.
Scans in Total	Displays the number of vulnerability scans. Click Scan to manually scan for vulnerabilities on servers.

- Viewing the importance of assets affected by a vulnerability
In the vulnerability list in the lower part of the page, view the importance of the asset affected by a vulnerability in the **Affected Servers** column.
 - : major asset
 - : minor asset
 - : test asset
- Viewing vulnerability details
Click the name of a target vulnerability. On the vulnerability details slide-out panel displayed, you can view the repair suggestions, CVE details, affected servers, and historical handling records of the vulnerability.
- Viewing handled vulnerabilities or vulnerabilities to be handled
Above the vulnerability list, select **Unhandled** or **Handled** from the vulnerability handling status drop-down list to filter vulnerabilities to be handled or that have been handled.
- Exporting the vulnerability list
Click **Export** above the vulnerability list to export vulnerability data with just one click. Then, you can view vulnerability information on your local PC.

 NOTE

A maximum of 30,000 vulnerabilities can be exported at a time.

- A maximum of 5,000 application vulnerabilities can be exported at a time.
- HSS automatically performs a comprehensive scan in the early morning every day. After the scan is complete, you can download the vulnerability report.


----End

Viewing Vulnerability Details (Server View)

 NOTE

The basic edition does not support this operation.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction > Vulnerabilities**.

Step 4 In the upper right corner of the **Vulnerabilities** page, click **Server view** to view vulnerability information.

- Viewing vulnerability scan results

In the vulnerability statistics area in the upper part of the **Vulnerabilities** page, view vulnerability scan results. [Table 5-5](#) describes related parameters.

Table 5-5 Vulnerability scan parameters

Parameter	Description
Critical vulnerabilities	Click the number in Critical vulnerabilities . On the slide-out panel displayed, you can view all types of vulnerabilities to be urgently fixed.
Unfixed Vulnerabilities	Click the number in Unfixed Vulnerabilities . On the slide-out panel displayed, you can view all types of vulnerabilities that are not fixed.
Servers with Vulnerabilities	Displays the number of servers with vulnerabilities.
Vulnerabilities Handled Today	Click the number in Vulnerabilities Handled Today . On the slide-out panel displayed, you can view all types of vulnerabilities that have been handled today.
Vulnerabilities Handled in Total	Click the number in Vulnerabilities Handled in Total . On the slide-out panel displayed, you can view all types of vulnerabilities that have been handled.
Detectable Vulnerabilities	Displays the number of vulnerabilities that can be detected by HSS.

Parameter	Description
Scans in Total	Displays the number of vulnerability scans. Click Scan to manually scan for vulnerabilities on servers.

- Viewing server details and vulnerabilities on servers
 - a. Click the name of a target server. On the server details slide-out panel displayed, you can view details about the server and vulnerabilities on the server.
 - b. Click the name of a target vulnerability. On the vulnerability details slide-out panel displayed, you can view the CVE details, affected servers, and historical handling records of the vulnerability.
- Viewing handled vulnerabilities or vulnerabilities to be handled
Above the vulnerability list, select **Unhandled** or **Handled** from the vulnerability handling status drop-down list to filter vulnerabilities to be handled or that have been handled.
- Exporting the list of servers with vulnerabilities
Click **Export** above the vulnerability list to export vulnerability data with just one click. Then, you can view vulnerability information on your local PC.

 **NOTE**

- A maximum of 30,000 vulnerabilities can be exported at a time.
- A maximum of 5,000 application vulnerabilities can be exported at a time.
 - HSS automatically performs a comprehensive scan in the early morning every day. After the scan is complete, you can download the vulnerability report.

----End

5.1.4 Fixing and Verifying the Fix of Vulnerabilities

- Linux or Windows vulnerabilities
You can select servers and click **Handle** to fix the vulnerabilities, 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.
- Application vulnerabilities
Manually fix them based on the suggestions provided on the page.

Constraints

- The **Server Status** is **Running**, **Agent Status** is **Online**, and **Protection Status** is **Protected**.

Precautions

- Vulnerability fixing operations cannot be rolled back. If a vulnerability fails to be fixed, services will probably be interrupted, and incompatibility issues will probably occur in middleware or upper layer applications. To prevent unexpected consequences, you are advised to use CBR to back up ECSs. 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.

Vulnerability Fix Priority

HSS' vulnerability scan system classifies vulnerability fix priorities into four levels: critical, high, medium, and low. You can refer to the priorities to fix the vulnerabilities that have significant impact on your server first.

- **Critical:** This vulnerability must be fixed immediately. Attackers may exploit this vulnerability to cause great damage to the server.
- **High:** This vulnerability must be fixed as soon as possible. Attackers may exploit this vulnerability to damage the server.
- **Medium:** You are advised to fix the vulnerability to enhance your server security.
- **Low:** This vulnerability has a small threat to server security. You can choose to fix or ignore it.

Vulnerability Display


Detected vulnerabilities will be displayed in the vulnerability list for seven days, regardless of whether you have handled them.

Automatically Fixing Vulnerabilities (Vulnerability View)

You can only fix Linux and Windows vulnerabilities with one click on the console.

NOTE

A maximum of 1,000 server vulnerabilities can be fixed at a time. If there are more than 1,000 vulnerabilities, fix them in batches.

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security** > Host Security Service.
- Step 3** In the navigation pane, choose **Prediction** > **Vulnerabilities**.
- Step 4** On the **Vulnerabilities** page displayed, locate the vulnerabilities you want to fix and fix the servers with the vulnerabilities.

- Fixing all servers affected by a vulnerability
Locate the row containing a target vulnerability and click **Fix** in the **Operation** column. Alternatively, you can select all target vulnerabilities and click **Fix** in the upper left corner of the vulnerability list to fix vulnerabilities in batches.
- Fixing one or more servers affected by a vulnerability
 - a. Click a vulnerability name.
 - b. On the vulnerability details slide-out panel displayed, click the **Affected** tab, locate the row containing the target server, and click **Fix** in the **Operation** column.
You can also select all target servers and click **Fix** above the server list to fix vulnerabilities for the servers in batches.

Step 5 In the **Fix** dialog box displayed, select **I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.** and click **Auto Fix**.

Step 6 Click a vulnerability name.

Step 7 Click the **Handling History** tab to view the fix status of the target vulnerability in the **Status** column. [Table 5-6](#) describes vulnerability fix statuses.

Table 5-6 Vulnerability fix statuses


Status	Description
Unhandled	The vulnerability is not fixed.
Ignored	The vulnerability does not affect your services. You have ignored the vulnerability.
Verifying	HSS is verifying whether a fixed vulnerability is successfully fixed.
Fixing	HSS is fixing the vulnerability.
Fixed	The vulnerability has been successfully fixed.
Restart required	The vulnerability has been successfully fixed. You need to restart the server as soon as possible.
Failed	The vulnerability fails to be fixed. The possible cause is that the vulnerability does not exist or has been changed.
Restart the server and try again	This status is displayed only for vulnerabilities that exist on Windows servers. The vulnerability has not been fixed on the Windows server for a long time. As a result, the latest patch cannot be installed. You need to install an earlier patch, restart the server, and then install the latest patch.

----End

Automatically Fixing Vulnerabilities (Server View)

You can only fix Linux and Windows vulnerabilities with one click on the console.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 Fix the vulnerability for a target server.

- Fixing all vulnerabilities on a server
 - a. Locate the row containing a target server and click **Fix** in the **Operation** column.
 - b. In the **Fix** dialog box displayed, select the type of the vulnerability to be fixed, select **I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.**, and click **OK**.

Only Linux and Windows vulnerabilities can be automatically fixed with one click. Web-CMS and application vulnerabilities need to be manually fixed by logging in to the server.
 - c. Click the server name. On the server details slide-out panel displayed, view the vulnerability fix status. [Table 5-7](#) describes vulnerability fix statuses.
- Fixing one or more vulnerabilities on a server
 - a. Click the name of a target server. The server details slide-out panel is displayed.
 - b. Locate the row containing a target vulnerability and click **Fix** in the **Operation** column.

Alternatively, you can select all target vulnerabilities and click **Fix** above the vulnerability list to fix vulnerabilities in batches.
 - c. In the **Fix** dialog box displayed, select **I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.**, and click **Auto Fix**.
 - d. In the **Status** column of the target vulnerability, view the fix status of the vulnerability. [Table 5-7](#) describes vulnerability fix statuses.

Table 5-7 Vulnerability fix statuses

Status	Description
Unhandled	The vulnerability is not fixed.
Ignored	The vulnerability does not affect your services. You have ignored the vulnerability.
Verifying	HSS is verifying whether a fixed vulnerability is successfully fixed.


Status	Description
Fixing	HSS is fixing the vulnerability.
Fixed	The vulnerability has been successfully fixed.
Restart required	The vulnerability has been successfully fixed. You need to restart the server as soon as possible.
Failed	The vulnerability fails to be fixed. The possible cause is that the vulnerability does not exist or has been changed.
Restart the server and try again	This status is displayed only for vulnerabilities that exist on Windows servers. The vulnerability has not been fixed on the Windows server for a long time. As a result, the latest patch cannot be installed. You need to install an earlier patch, restart the server, and then install the latest patch.

----End

Manually Fixing Vulnerabilities

HSS does not automatically fix Web-CMS or application vulnerabilities with one click. You can log in to the server to manually fix them by referring to the fix suggestions on the vulnerability details slide-out panel.

Viewing vulnerability fix suggestions

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security** > Host Security Service.
- Step 3** In the navigation pane, choose **Prediction** > **Vulnerabilities**.
- Step 4** Click the name of a target vulnerability to access the vulnerability details slide-out panel and view the fix suggestions.

----End

Fixing vulnerabilities by referring to vulnerability fix suggestions

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

- Method 1: Create a new VM to fix the vulnerability.
 - a. Create an image for the ECS to be fixed.
 - b. Use the image to create an ECS.
 - c. Fix the vulnerability on the new ECS and verify the result.
 - d. Switch services over to the new ECS and verify they are stably running.
 - e. Release the original ECS. If a fault occurs after the service switchover and cannot be rectified, you can switch services back to the original ECS.

- Method 2: Fix the vulnerability on the target server.
 - a. Create a backup for the ECS whose vulnerabilities need to be fixed.
 - b. Fix vulnerabilities on the current server.
 - c. If services become unavailable after the vulnerability is fixed and cannot be recovered in a timely manner, use the backup to restore the server.

 **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.

After the vulnerability is ignored, no alarm will be generated for the vulnerability.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

Step 4 Locate the row containing a target vulnerability and click **Ignore** in the **Operation** column.


Step 5 In the dialog box displayed, click **OK**.

----End

Whitelisting Vulnerabilities

If you evaluate that some vulnerabilities do not affect your services and do not want to view the vulnerabilities in the vulnerability list, you can whitelist the vulnerabilities. After they are whitelisted, the vulnerabilities will be ignored in the vulnerability list and no alarms will be reported. The vulnerabilities will not be scanned and the vulnerability information will not be displayed when the next vulnerability scan task is executed.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction** > **Vulnerabilities**.

- Whitelisting all servers that are affected by a vulnerability
HSS will ignore the vulnerability when scanning for vulnerabilities on all servers.

- a. In the **Operation** column of the row containing the target vulnerability, click **More** and select **Add to Whitelist**.
You can also select multiple vulnerabilities and click **Add to Whitelist** above the vulnerability list.
- b. In the dialog box displayed, click **OK**.
- Whitelisting one or more servers that are affected by a vulnerability
HSS will ignore the vulnerability when scanning for vulnerabilities on these servers.
 - a. Click a target vulnerability name.
 - b. On the slide-out panel displayed, click the **Affected** tab.
 - c. In the **Operation** column of the row containing the target server, click **More** and select **Add to Whitelist**.
You can also select multiple servers and click **Add to Whitelist** above the server list.
 - d. In the dialog box displayed, click **OK**.
- Whitelisting vulnerabilities using whitelist rules
 - a. In the upper right corner of the **Vulnerabilities** page, click **Configure Policy**. The **Configure Policy** slide-out panel is displayed.
 - b. In the **Vulnerability Whitelist** area, click **Add Rule**.
 - c. Configure a whitelist rule according to [Table 5-8](#).

Table 5-8 Vulnerability whitelist rule parameters

Parameter	Description
Type	Select the type of vulnerabilities to be whitelisted. Possible values are as follows: <ul style="list-style-type: none">▪ Linux Vulnerabilities▪ Windows Vulnerabilities▪ Web-CMS Vulnerabilities▪ Application Vulnerabilities
Vulnerability	Select one or more vulnerabilities to be whitelisted.

Parameter	Description
Rule Scope	Select the servers affected by the vulnerabilities. Possible values are as follows: <ul style="list-style-type: none">▪ All servers HSS will ignore the vulnerability when scanning for vulnerabilities on all servers.▪ Selected servers Select one or more target servers. HSS will ignore the vulnerabilities when scanning for vulnerabilities on these servers. You can search for a target server by server name, ID, EIP, or private IP address.
Remarks (Optional)	Enter the remarks.

d. Click **OK**.

----End

Verifying 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 5-9 Verification commands

OS	Verification Command
CentOS/Fedora/ EulerOS/Red Hat/Oracle	<code>rpm -qa grep <i>Software_name</i></code>
Debian/Ubuntu	<code>dpkg -l grep <i>Software_name</i></code>
Gentoo	<code>emerge --search <i>Software_name</i></code>

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.

5.1.5 Managing the Vulnerability Whitelist


If you evaluate that some vulnerabilities do not affect your services and do not want to view the vulnerabilities in the vulnerability list, you can whitelist the

vulnerabilities. After they are whitelisted, the vulnerabilities will be ignored in the vulnerability list and no alarms will be reported. The vulnerabilities will not be scanned and the vulnerability information will not be displayed when the next vulnerability scan task is executed.

This section describes how to whitelist a vulnerability, modify a vulnerability whitelist rule, and remove a vulnerability whitelist rule from the vulnerability whitelist.

Whitelisting Vulnerabilities

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction > Vulnerabilities**.

- Whitelisting all servers that are affected by a vulnerability
HSS will ignore the vulnerability when scanning for vulnerabilities on all servers.
 - a. In the **Operation** column of the row containing the target vulnerability, click **More** and select **Add to Whitelist**.
You can also select multiple vulnerabilities and click **Add to Whitelist** above the vulnerability list.
 - b. In the dialog box displayed, click **OK**.
- Whitelisting one or more servers that are affected by a vulnerability
HSS will ignore the vulnerability when scanning for vulnerabilities on these servers.
 - a. Click a target vulnerability name.
 - b. On the slide-out panel displayed, click the **Affected** tab.
 - c. In the **Operation** column of the row containing the target server, click **More** and select **Add to Whitelist**.
You can also select multiple servers and click **Add to Whitelist** above the server list.
 - d. In the dialog box displayed, click **OK**.
- Whitelisting vulnerabilities using whitelist rules
 - a. In the upper right corner of the **Vulnerabilities** page, click **Configure Policy**. The **Configure Policy** slide-out panel is displayed.
 - b. In the **Vulnerability Whitelist** area, click **Add Rule**.
 - c. Configure a whitelist rule according to [Table 5-10](#).

Table 5-10 Vulnerability whitelist rule parameters


Parameter	Description
Type	Select the type of vulnerabilities to be whitelisted. Possible values are as follows: <ul style="list-style-type: none">▪ Linux Vulnerabilities▪ Windows Vulnerabilities▪ Web-CMS Vulnerabilities▪ Application Vulnerabilities
Vulnerability	Select one or more vulnerabilities to be whitelisted.
Rule Scope	Select the servers affected by the vulnerabilities. Possible values are as follows: <ul style="list-style-type: none">▪ All servers HSS will ignore the vulnerability when scanning for vulnerabilities on all servers.▪ Selected servers Select one or more target servers. HSS will ignore the vulnerabilities when scanning for vulnerabilities on these servers. You can search for a target server by server name, ID, EIP, or private IP address.
Remarks (Optional)	Enter the remarks.

d. Click **OK**.

----End

Editing a Vulnerability Whitelist

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prediction > Vulnerabilities**.


Step 4 In the upper right corner of the **Vulnerabilities** page, click **Configure Policy**. The **Configure Policy** slide-out panel is displayed.

Step 5 In the row containing the desired vulnerability whitelist rule, click **Edit** in the **Operation** column.

Step 6 On the editing page, modify the information and click **OK**.

----End

Removing a Vulnerability Whitelist Rule from the Vulnerability Whitelist


- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Prediction > Vulnerabilities**.
- Step 4** In the upper right corner of the **Vulnerabilities** page, click **Configure Policy**. The **Configure Policy** slide-out panel is displayed.
- Step 5** In the row containing the desired vulnerability whitelist rule, click **Delete** in the **Operation** column.
- Step 6** In the dialog box displayed, confirm the information and click **OK**.

----End

5.1.6 Viewing Vulnerability Handling History


For vulnerabilities that have been handled, you can refer to this section to view the vulnerability handling history (handler and handling time).


Viewing the Handling History of a Vulnerability

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Prediction > Vulnerabilities**.
- Step 4** In the list of handled vulnerabilities, click a vulnerability name. The vulnerability details slide-out panel is displayed.
- Step 5** Click the **Handling History** tab to view the handling history of the vulnerability.

----End

Viewing the Handling History of all Vulnerabilities

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane on the left, choose **Security Operations > Handling History**. The **Handling History** page is displayed.
- Step 4** On the **Vulnerabilities** tab page displayed, view the handling history of all vulnerabilities.
 - Viewing the vulnerability handling history of a specified property

In the search box above the vulnerability handling history list, enter a vulnerability type, vulnerability name, or server IP address, and click  to view the vulnerability handling history of a specified property.

----End

5.2 Baseline Inspection

5.2.1 Baseline Check Overview

HSS detects complex policies, weak passwords, and configuration details, including the safe settings rate, top 5 servers with unsafe settings, servers with weak passwords, and top 5 servers with weak passwords. HSS proactively checks weak password complexity policies and other unsafe settings, and provides [suggestions](#) for fixing detected risks.

Constraints

Servers that are not protected by HSS do not support baseline-related operations.

Prerequisite

Only the servers protected by the enterprise edition or above are checked.

Check Methods


- Automatic check
HSS automatically performs a comprehensive check at 04:00 every day. If you want to customize the automatic baseline check period and time, you can enable premium, WTP, and container editions. For details, see [Configuration Check](#).
- Manual check
To view the baseline risks of a specified server, you can [create a baseline check policy](#) for these servers. In the upper right corner of the **Baseline Checks** page, select a policy and click **Scan**. After the manual baseline check is complete, you can view the baseline risks of specified servers.

Check Items

Item	Description
Password Complexity Policy Detection	Check password complexity policies and modify them based on suggestions provided by HSS to improve password security.
Common Weak Password Detection	Change weak passwords to stronger ones based on HSS scan results and suggestions.

Unsafe Configurations	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.
-----------------------	--

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane on the left, choose **Prediction > Baseline Checks**.
- Step 4** Click different tabs on the displayed page to check detected unsafe configurations. [Table 5-11](#) lists the corresponding parameters.

To view the check results of servers under different baseline check policies, you can switch between baseline check policies.

Table 5-11 Baseline check overview

Parameter	Description
Baseline Check Policy	Available baseline check policies that have been added. You can select, create, edit, and delete these policies.
Scanned Servers	Total number of detected servers.
Security Baselines	Number of baselines executed during the server detection.
Baseline Check Items	Total number of checked server configuration items.
Safe Settings Rate	Percentage of configuration items that passed the baseline check to the total number of check items. Failed items are displayed by risk level.
Top 5 Servers with Unsafe Settings	Statistics on servers with server configuration risks. The top 5 servers with the highest risks are preferentially sorted. If no high-risk settings exist, the servers are sorted into medium-risk and low-risk ones in sequence.
Servers with Weak Passwords	Total number of detected servers, as well as the numbers of servers with weak passwords, those without weak passwords, and those with weak password detection disabled.
Top 5 Servers with Weak Passwords	Statistics on the top 5 servers with most weak password risks.
Unsafe Configurations	Alarms generated for servers with configuration risks and the risk statistics.

Parameter	Description
Password Complexity Policy Detection	Statistics on servers with weak passwords that do not meet the baseline requirements.
Common Weak Password Detection	Statistics on servers with weak passwords and accounts.

----End

Manually Performing a Baseline Check

NOTICE

- In a manual check, only the servers associated with the target baseline policy are checked. If the default policy is used, [associate servers](#) and then perform the manual check.
- Before performing a manual check, check whether the target policy is available in the **Baseline Check Policy** drop-down list. For details about how to create a policy, see [Creating a Baseline Check Policy](#).

Step 1 Choose **Prediction > Baseline Checks**. Select the target baseline check policy.

Step 2 Click **Scan** in the upper right corner of the page.

Step 3 If the time displayed in the **Last scanned** area under the **Baseline Check Policy** is the actual check time, the check is complete.

NOTE


- After a manual check is performed, the button will display **Scanning** and be disabled. If the check time exceeds 30 minutes, the button will be automatically enabled again. If the time displayed in the **Last scanned** area becomes the current check time, it indicates the check has completed.
- After the check is complete, you can view the check results and handling suggestions by referring to [Viewing Baseline Check Details](#).

----End

Exporting the Baseline Check Report

You can filter and export the baseline check report as required.

Step 1 Log in to the management console.


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

Step 3 In the navigation pane on the left, choose **Prediction > Baseline Checks**.

Step 4 Click different tabs on the displayed page to check the detected risks.

 NOTE

Currently, only reports on the **Unsafe Configurations** and **Common Weak Password Detection** pages can be exported.

Step 5 Click the **Unsafe Configurations** or **Common Weak Password Detection** tab and click  in the upper right corner of the list to download the filtered risk alarms.

 NOTE

- On the **Unsafe Configurations** page, you can click the image in the corresponding column to search for alarms based on risk level and type.
- On the **Common Weak Password Detection** tab, you can search for alarms by server name, IP address, and account name, and download the alarms.
- A maximum of 5,000 risk check reports can be downloaded at a time from the **Unsafe Configurations** and **Common Weak Password Detection** pages.

----End

5.2.2 Viewing Baseline Check Details

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

Constraints

Servers that are not protected by HSS do not support baseline-related operations.

Prerequisite

Only the servers protected by the enterprise edition or above are checked.

Detection Description

The MySQL baseline detection of Linux OS is based on the MySQL 5 security configuration specifications. If MySQL 8 is installed on your server, the following check items are not displayed in the detection results, because they are discarded in that version. The detection results are displayed only on the server whose MySQL version is 5.

- Rule: Do not set **old_passwords** to 1.
- Rule: Set **secure_auth** to 1 or ON.
- Rule: Do not set **skip_secure_auth**.
- Rule: Set **log_warnings** to 2.
- Rule: Configure the MySQL binlog clearing policy.
- Rule: The **sql_mode** parameter contains **NO_AUTO_CREATE_USER**.
- Rule: Use the MySQL audit plug-in.

Check Items


Table 5-12 Check items

Item	Description
Unsafe configurations	Currently, the following check standards and types are supported: <ul style="list-style-type: none">• For Linux:<ul style="list-style-type: none">– Huawei Cloud security practices: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 7, EulerOS, EulerOS_ext, Kubernetes-Node, and Kubernetes-Master.– DJCP MLPS compliance: Apache 2, MongoDB, MySQL 5, Nginx, Tomcat, CentOS 6, CentOS 7, CentOS 8, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, Alma.• For Windows:<ul style="list-style-type: none">– The cloud security practice baseline can check MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008, Windows_2012, Windows_2016, and Windows_2019.
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.

Viewing Unsafe Configurations

View the risk statistics of unsafe configurations and the corresponding suggestions.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Prediction > Baseline Checks**.

Step 4 Click the **Unsafe Configurations** tab to view the risk items. For more information, see [Table 5-13](#).

To view the server configuration check results under a specified baseline check policy, select a policy in the **Baseline Check Policy** drop-down list.

Table 5-13 Parameter description

Parameter	Description
Risk Level	Level of a detection result. <ul style="list-style-type: none">• High• Low• Medium• Safe
Baseline Name	Name of the baseline that is checked.
Type	Policy type of the baseline that has been checked. <ul style="list-style-type: none">• Cloud security practices• DJCP MLPS
Check Item	Total number of configuration items that are checked.
Risky Item	Total number of the risky configurations.
Affected Servers	Total number of servers affected by the detected risks in a baseline.
Last Scanned	Time when the last detection was performed.
Description	Description of a baseline.

Step 5 Click the target baseline name in the list to view the baseline description, affected servers, and details about all check items.

Step 6 Click **View Details** in the **Operation** column of the target check item to view the description, audit description, and handling suggestions.

You need to check whether a risk item is critical or need to be handled.

If yes, modify the check item according to the handling suggestions. If no, click **Ignore** in the **Operation** column of the check item.

----End

Viewing Password Complexity Policy Detection

View the risk statistics and handling suggestions of password complexity policy detection.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Prediction > Baseline Checks**.

Step 3 Click the **Password Complexity Policy Detection** tab to view the risk statistical items and handling suggestions. For more information, see [Table 5-14](#).

Table 5-14 Parameter description

Parameter	Description
Server	Name and IP address of the detected server.
Password Length	Whether the password length of the target server meets the requirements. <ul style="list-style-type: none">• Passed• Failed
Uppercase Letters	Whether the uppercase letters used in the target server password meet the requirements. <ul style="list-style-type: none">• Passed• Failed
Lowercase Letters	Whether the lowercase letters used in the target server password meet the requirements. <ul style="list-style-type: none">• Passed• Failed
Digits	Whether the digits used in the target server password meet the requirements. <ul style="list-style-type: none">• Passed• Failed
Special characters	Whether the special characters used in the target server password meet the requirements. <ul style="list-style-type: none">• Passed• Failed
Suggestion	Suggestion for fixing unsafe passwords

----End

Viewing Common Weak Password Detection

View the risk statistics of weak password detection and the corresponding handling suggestions.

- Step 1** Log in to the management console and go to the HSS page.
- Step 2** In the navigation pane on the left, choose **Prediction > Baseline Checks**.
- Step 3** Click the **Common Weak Password Detection** tab to view the statistics of risky weak password accounts on the server. For more information, see [Table 5-15](#).

Table 5-15 Parameter description

Parameter	Description
Server	Name and IP address of the detected server.
Account Name	Accounts with weak passwords that are detected on the target server.
Account Type	Type of an account.
Usage Duration (Days)	Period for using a weak password.

NOTE


- 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.

- A password should contain more than eight characters, including uppercase letters, lowercase letters, digits, and special characters.

----End

Exporting the Baseline Check Report

On the **Baseline Checks** page, you can click  in the upper right corner of a tab to export the check report.

NOTE

- The check result of a single cloud server cannot be separately exported.
- Up to 5000 alarm records can be exported at a time.

5.2.3 Fixing Unsafe Settings

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

Constraints

Servers that are not protected by HSS do not support baseline-related operations.

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, perform a manual check in the upper part of the **Baseline Checks** page to verify the result. If you do not perform a manual verification, HSS will automatically check the settings at 00:00:00 the next day.

Improving Password Strength

- 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 manually check the result immediately. If you do not perform a manual verification, HSS will automatically check the settings at 00:00:00 the next day.

Fixing Unsafe Configurations on a Server

Unsafe configurations in key applications in the host system may be exploited by hackers to intrude the system. Such configurations include insecure encryption algorithms used by SSH and Tomcat startup with root permissions.

HSS can detect unsafe configurations provide detailed suggestions.

Step 1 On the HSS console, choose **Asset Management > Servers & Quota** and click the **Servers** tab.

Step 2 Search for the target server and click the server name to go to the server details page.

Step 3 Click the **Baseline Checks** and click the **Unsafe Configurations** tab. Click the icon before a risk item to expand and view all check item details.

Step 4 Handle risk items.

- Ignoring risks

Click **Ignore** in the **Operation** column of the target check item to ignore a check item.

Select multiple check items and click **Ignore** to ignore them in batches.

- Fixing risks

a. Click **View Details** in the **Operation** column of the target risk item to view the check item details.

b. View the content in the **Audit Description** and **Suggestion** and rectify the unsafe configurations.

 NOTE

- You are advised to fix the settings with high severity immediately and fix those with medium or low severity.
- Verification
If a failed check item has been fixed, you can update its status through verification.
If a check item failed to be fixed, click **View Cause** to view the cause. Then, fix it again.

 NOTE

- Currently, baseline checks are not supported for Windows OSs.
 - The agent status of the target server must be online.
 - Only one risk item can be verified at a time. Other risk items can be verified only after the risk items are verified.
 - Baseline checks are supported for the following Linux OSs: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftpd, CentOS 6, CentOS 7, CentOS 8, EulerOS, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, and Ubuntu 18.
- a. Click **Verify** in the **Operation** column of the row that contains the target risk item.
 - b. In the displayed dialog box, click **OK**. The status changes to **Verifying**. The system starts automatic verification. After the verification is complete, check the status.


----End

Fixing Risky Configurations on all Servers

Risky configurations in key applications in the host system may be exploited by hackers to intrude the system. Such configurations include insecure encryption algorithms used by SSH and Tomcat startup with root permissions.

HSS can detect unsafe configurations provide detailed suggestions.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Prediction > Baseline Checks**.

Step 4 Click the **Unsafe Configurations** tab to view the risk items. For more information, see [Table 5-16](#).

To view the server configuration check results under a specified baseline check policy, select a policy in the **Baseline Check Policy** drop-down list.

Table 5-16 Parameter description

Parameter	Description
Risk Level	Level of a detection result. <ul style="list-style-type: none">• High• Low• Medium• Safe
Baseline Name	Name of the baseline that is checked.
Type	Policy type of the baseline that has been checked. <ul style="list-style-type: none">• Cloud security practices• DJCP MLPS
Check Item	Total number of configuration items that are checked.
Risky Item	Total number of the risky configurations.
Affected Servers	Total number of servers affected by the detected risks in a baseline.
Last Scanned	Time when the last detection was performed.
Description	Description of a baseline.

Step 5 Click the target baseline name in the list to view the baseline description, affected servers, and details about all check items.

Step 6 Handle risk items.

- Ignoring risks
 - Click **Ignore** in the **Operation** column of the target check item to ignore a check item.
 - Select multiple check items and click **Ignore** to ignore them in batches.
- Fixing risks
 - Click **View Details** in the **Operation** column of the target risk item to view the check item details.
 - View content in the **Audit Description** and **Suggestion** text boxes, and handle the risks based on the suggestions or **Expected Result** described in the **Test Cases** area.

 NOTE

- Currently, one-click fixing is supported for some EulerOS baseline configurations and CentOS 8 baseline configurations. You can simply click **Fix** in the **Operation** column of the target EulerOS or CentOS check item to fix the unsafe configurations. If some parameters need to be configured during restoration, retain the default values.
 - You are advised to fix the settings with high severity immediately and fix those with medium or low severity.
- c. Click **Affected Servers** to view the servers affected by the check item. Click **Verify** to update the list of affected servers.
- Verification
- If a failed check item has been fixed, you can update its status through verification.
- If a check item failed to be fixed, click **View Cause** to view the cause. Then, fix it again.

 NOTE

- Currently, baseline checks are not supported for Windows OSs.
 - The agent status of the target server must be online.
 - Only one risk item can be verified at a time. Other risk items can be verified only after the risk items are verified.
 - Baseline checks are supported for the following Linux OSs: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftpd, CentOS 6, CentOS 7, CentOS 8, EulerOS, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, and Ubuntu 18.
- a. Click **Verify** in the **Operation** column of the row that contains the target risk item.
- b. In the displayed dialog box, click **OK**. The status changes to **Verifying**. The system starts automatic verification. After the verification is complete, check the status.

----End

5.2.4 Managing Baseline Check Policies


You can create, edit, and delete check policies for manual baseline checks, and can customize check item as required.

Constraints

- The policies on the **Prediction > Baseline Checks** page only take effect on manual baseline checks. For details about how to configure the policies, see "Configuration Check" and "Weak Password Scan" in [Modifying a Policy](#).
- Servers that are not protected by HSS do not support baseline-related operations.

Creating a Baseline Check Policy

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Prediction > Baseline Checks**.

Step 4 Click **Policies** in the upper right corner of the page.

Step 5 Click **Create Policy** and configure the policy information by referring to [Table 5-17](#).

To check baseline details, click **Rule Details** on the right of a baseline name.

 **NOTE**

If you select **Linux** for **OS**, you can select any checks included in **Baseline** and edit rules. This function is not supported for Windows servers.

Table 5-17 Baseline policy parameters

Parameter	Description	Example Value
Policy Name	Policy name	linux_web1_security_policy
OS	OS that will be checked. <ul style="list-style-type: none"> Linux Windows 	Linux
Baseline	Baseline used for a check. Check items are as follows: <ul style="list-style-type: none"> For Linux: <ul style="list-style-type: none"> Huawei Cloud security practices: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftpd, CentOS 7, EulerOS, EulerOS_ext, Kubernetes-Node, and Kubernetes-Master. DJCP MLPS compliance: Apache 2, MongoDB, MySQL 5, Nginx, Tomcat, CentOS 6, CentOS 7, CentOS 8, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, Alma. For Windows: <ul style="list-style-type: none"> The cloud security practice baseline can check MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008, Windows_2012, Windows_2016, and Windows_2019. 	Cloud security practices: Select all. DJCP MLPS: Select all.

- Step 6** Confirm the information, click **Next**, and select the server to be associated with the application based on the server name, server ID, EIP, or private IP address.
- Step 7** Confirm the information and click **OK**. The baseline policy will be displayed in the policy list.
- End

Editing a Baseline Check Policy

- Step 1** Log in to the HSS management console.
- Step 2** In the navigation pane on the left, choose **Prediction > Baseline Checks**.
- Step 3** Click **Policies** in the upper right corner of the page.
- Step 4** Click **Edit** in the **Operation** column of a policy. On the policy details page that is displayed, configure the policy name and check items.

NOTE

If you select **Linux** for **OS**, you can select any checks included in **Baseline** and edit rules. This function is not supported for Windows servers.

- Step 5** Confirm the configuration, click **Next**, and select servers.
- Step 6** Confirm the information and click **OK**. You can view the updated policy in the policy list.
- End

Deleting a Baseline Check Policy

- Step 1** Log in to the HSS management console.
- Step 2** In the navigation pane on the left, choose **Prediction > Baseline Checks**.
- Step 3** Click **Policies** in the upper right corner of the page.
- Step 4** Click **Delete** in the **Operation** column of a policy. In the dialog box that is displayed, confirm the information and click **OK**.
- End

5.3 Container Image Security

5.3.1 Image Vulnerabilities

This section describes how to check the vulnerabilities on the private image and determine whether to ignore the vulnerabilities.

Prerequisites

Container protection has been enabled.

Detection Method

After you enable node protection, your Linux images will be scanned automatically.

Constraints

Only vulnerabilities in Linux images can be checked.

Viewing Vulnerabilities in Private Images


Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Prediction > Container Images**. On the displayed page, click **Image Vulnerabilities** and click **Private Image Vulnerabilities** to view private image vulnerabilities.

NOTE

Click a risky image to check its vulnerability overview, including the vulnerability name, urgency, status, the number of affected images, and vulnerability description.

Table 5-18 Parameter description

Parameter	Description	Operation
Vulnerability Name	-	<ul style="list-style-type: none">Click  to view the details of a vulnerability, including CVE ID, CVSS Score, Disclosed, and Vulnerability Details.Click the name of a vulnerability to view the images affected by the vulnerability. For details, see Step 3.
Repair Urgency	Shows whether the vulnerability should be repaired immediately.	-
Historically Affected Images	Shows the number of images that have been affected.	-
Solution	Provides a solution to fix the vulnerability.	Click the link in the Solution column to view the solution.

Step 3 Click the vulnerability name to view its basic information and affected images.

----End

5.3.2 Viewing Malicious File Detection Results

Malicious files in the private images can be automatically detected, helping you discover and eliminate the security threats in your assets.

Check Frequency

A comprehensive check is automatically performed in the early morning every day.


Prerequisites

Container protection has been enabled.

Constraints

Only malicious files in Linux images can be detected.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation tree on the left, choose **Prediction > Container Images**.
- Step 4** Click the **Malicious Files** tab to view details about the malicious files in private images. Delete the malicious files or create images again as needed based on the scan result.
 - Malicious files include Trojans, worms, viruses, and Adware.
 - In the **Image Tag** column, click an image version to view its vulnerability report.

----End

5.3.3 Image Baseline Check

Your private image repository is scanned for unsafe configurations and provides suggestions for modifying the configurations, helping you fight intrusions and meet compliance requirements.

Check Frequency

A comprehensive check is automatically performed by HSS in the early morning every day.

Prerequisites

Container protection has been enabled.

Constraints

Only configuration risks in Linux images can be detected.


Check Items

- Accounts with duplicate names or UIDs
- Non-root accounts whose UIDs are 0

- Password check in code
- Accounts with duplicate password hash values
- Weak password hash algorithms
- Ensuring that the account password is not empty.
- Duplicate group names or GIDs
- Non-privileged account incorrectly included in the privilege group
- Old "+" entries in the /etc/passwd file
- Old "+" entries in the /etc/shadow file
- Old "+" entries in the /etc/group file
- Ensuring all groups in the /etc/passwd file are in the /etc/group file
- Unconfigured password validity period
- Ensuring that the password change dates of all users are past dates.
- Host trust relationship
- Preset root-level trust relationship establishment
- User **root** not in the group with GID 0
- Members in the shadow group


Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Prediction** > **Container Images**.

Step 4 Click the **Unsafe Settings** tab to view the unsafe settings in the image.

Step 5 Click  next to a check item to view its details and suggestions, and modify your unsafe settings accordingly.

----End

6 Prevention

6.1 Application Protection

6.1.1 Viewing Application Protection

To protect your applications with RASP, you simply need to add probes to them, without having to modify application files.

Technical Principles

Probes (monitoring and protection code) are added to the checkpoints (key functions) of applications through dynamic code injection. The probes identify attacks based on predefined rules, data passing through the checkpoints, and contexts (application logic, configurations, data, and event flows).

Prerequisites


You have enabled HSS premium, WTP, or container edition.

Constraints

- Currently, only Linux servers are supported.
- So far, only Java applications can be protected.
- The premium and higher editions support operations related to application protection.

Viewing Protection Settings

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Application Protection**. Click the **Protected Servers** tab.

- Step 4** Click the **Protection Servers** tab and check the server list. The server parameters are as follows.

Table 6-1 Parameter description

Parameter	Description
Server Name/ID	Server name and ID
IP Address	Private IP address and EIP of the server
OS	Server OS
Server Group	Group that the server belongs to
Policy	Detection policies bound to the target server.
Protection Status	Protection status of a server <ul style="list-style-type: none">● Protected● Unprotected
Microservice Protection	Microservice protection status. Its value can be: <ul style="list-style-type: none">● Active● Installing● Configuration pending● Installation failed
RASP Protection.	RASP protection status. Its value can be: <ul style="list-style-type: none">● Installing● Configuration pending● Installation failed
Detected Attacks	Number of attacks detected by RASP.

----End

Viewing Events

- Step 1** Log in to the management console and go to the HSS page.
- Step 2** Choose **Prevention > Application Protection** and click the **Events** tab. For details about the parameters, see [Table 6-2](#).

Table 6-2 Event parameters

Parameter	Description
Severity	Alarm severity
Server Name	Server that triggers an alarm
Alarm Name	Alarm name

Parameter	Description
Alarm Time	Time when an alarm is reported
Attack Source IP Address	IP address of the server that triggers the alarm
Attack Source URL	URL of the server that triggers the alarm

Step 3 You can click an alarm name to view the attack information (such as the request information and attack source IP address) and extended information (such as detection rule ID and description), and troubleshoot the problem accordingly.

----End

6.1.2 Enabling Application Protection

Prerequisites


You have enabled HSS premium, WTP, or container edition.

Constraints

- Currently, only Linux servers are supported.
- So far, only Java applications can be protected.
- The premium and higher editions support operations related to application protection.

Procedure

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Application Protection**. Click the **Protected Servers** tab.

Step 4 Click **Add Server**. Select servers in the dialog box that is displayed.

NOTE

You can select a default security policy or create a security policy.

Step 5 Click **Add and Enable Protection**.

Step 6 On the **Protected Servers** tab, click the status in the **RASP Protection** column.

Step 7 Check the RASP software installation progress. Wait until the message "Installation completed." is displayed.

Step 8 Log in to the server, go to the Spring Boot startup path, and copy the parameters from the **Configure Startup Parameters** step to the command box.

Step 9 Restart the microservice to apply the protection settings.

Step 10 On the **Protected Servers** tab, check the protection status in the **Microservice Protection** column. If the status is **Active**, the protection has been enabled.

----End

6.1.3 Managing Application Protection

Prerequisites


You have enabled HSS premium, WTP, or container edition.

Constraints

- Currently, only Linux servers are supported.
- So far, only Java applications can be protected.
- The premium and higher editions support operations related to application protection.

Viewing the Report

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Application Protection**. Click the **Protected Servers** tab.

Step 4 Click **View Report** in the **Operation** column of a server to view detection details.

Step 5 Click an alarm name to view its details.

You can view the attack information (such as the request information and attack source IP address) and extended information (such as detection rules and probes), and troubleshoot the problem accordingly.

----End

6.1.4 Disabling Application Protection

Prerequisites


You have enabled HSS premium, WTP, or container edition.

Constraints


- Currently, only Linux servers are supported.
- So far, only Java applications can be protected.
- The premium and higher editions support operations related to application protection.

Procedure

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Application Protection**. Click the **Protected Servers** tab.

Step 4 Toggle off the  switch in the **RASP Protection** column or click **Disable Protection** in the **Operation** column.

Step 5 In the dialog box that is displayed, confirm the server information and click **OK**.

 **NOTE**

After RASP is disabled for a server, the server will be removed from the **Protected Servers** tab. For details about how to enable protection, see [Enabling Application Protection](#).

----End

6.1.5 Managing Policies


You can add, edit, and delete application protection policies, and select and configure detection rules for the policies.

Constraints

- Currently, only Linux servers are supported.
- So far, only Java applications can be protected.
- You have enabled HSS premium, WTP, or container edition.

Adding a Protection Policy

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Application Protection** and click **Protection Policies**. For details about the parameters, see [Table 6-3](#).

Table 6-3 Protection policy parameters

Parameter	Description
Policy Name	Protection policy name
Detection Rule	Detection rules supported by a policy.
Associated Servers	Number of servers bound to a policy.

Step 4 Click **Add Policy**. In the dialog box that is displayed, enter the policy name, select the rules to be detected, and configure details about some detection rules. For details about the parameters, see [Table 6-4](#).

Table 6-4 Application protection policy parameters

Parameter	Description
Policy Name	User-defined policy name
Enabled	Whether to enable a detection rule for the current policy. You can select detection rules to enable them as required.
Detection Rule ID	ID of a detection rule
Action	Protection action of a detection rule. <ul style="list-style-type: none">• Detect: Detects objects based on the target rule and reports alarms for detected risk events.• Detect and block: Detects objects based on the target rule, reports alarms for detected risk events, and directly blocks or intercepts detected risk items. NOTICE Blocking or interception may interrupt services. Exercise caution when enabling this function
Description	Description about the detected object and behavior of the target protection policy.

Step 5 Click **Configure** in the **Operation** column of a detection rule to modify the rule content. [Table 6-5](#) describes the supported detection rules.

Table 6-5 Detection rules that can be configured

Rule	Description	Example
XXE	User-defined XXE blacklist protocol	.xml;.dtd;
XSS	User-defined XSS shielding rules	xml;doctype;xmlns;import;entity
WebShellUpload	User-defined suffix of files in the blacklist.	.jspx;.jsp;.jar;.phtml;.asp;.php;.aspx;.ashx;.cer
FileDirAccess	User-defined path of files in the blacklist.	/etc/passwd;/etc/shadow;/etc/gshadow;

Step 6 Confirm the configured policy and selected detection rules, and click **OK**. You can check whether the rule is added on the **Protection Policy** tab page.

----End

Editing a Protection Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Prevention > Application Protection** and click **Protection Policies**. For details about the parameters, see [Table 6-6](#).

Table 6-6 Protection policy parameters

Parameter	Description
Policy Name	Protection policy name
Detection Rule	Detection rules supported by a policy.
Associated Servers	Number of servers bound to a policy.

Step 3 Click **Edit** in the **Operation** column of a policy to configure the policy name, supported detection rules, and rule content.

Table 6-7 Application protection policy parameters

Parameter	Description
Policy Name	User-defined policy name
Enabled	Whether to enable a detection rule for the current policy. You can select detection rules to enable them as required.
Detection Rule ID	ID of a detection rule
Action	Protection action of a detection rule. <ul style="list-style-type: none">• Detect: Detects objects based on the target rule and reports alarms for detected risk events.• Detect and block: Detects objects based on the target rule, reports alarms for detected risk events, and directly blocks or intercepts detected risk items. NOTICE Blocking or interception may interrupt services. Exercise caution when enabling this function
Description	Description about the detected object and behavior of the target protection policy.

Step 4 Confirm the configured rule and selected detection items and click **OK**. You can check whether the target policy is modified on the **Protection Policy** tab page.

----End

Deleting a Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 Choose **Prevention > Application Protection** and click **Protection Policies**. For details about the parameters, see [Table 6-8](#).

Table 6-8 Protection policy parameters

Parameter	Description
Policy Name	Protection policy name
Detection Rule	Detection rules supported by a policy.
Associated Servers	Number of servers bound to a policy.

Step 3 Click **Delete** in the **Operation** column of the target policy. In the dialog box that is displayed, confirm the policy information and click **OK**.

NOTICE

If the policy to be deleted is associated with a server, bind the server to another protection policy first. Otherwise, the **Delete** button of the target policy is hidden.

----End

6.2 WTP

6.2.1 Adding a Protected Directory

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

Prerequisites

You have enabled the WTP edition.


Constraints and Limitations

- Only the servers that are protected by the HSS WTP edition support the operations described in this section.
- The constraints on protected directories are as follows:
 - For Linux,
 - A server can have up to 50 protected directories.
 - The complete path of a protected directory cannot exceed 256 characters.
 - The folder levels of a protected directory cannot exceed 100.
 - The total folders in protected directories cannot exceed 900,000.
 - For Windows,
 - A server can have up to 50 protected directories.

- The complete path of a protected directory cannot exceed 256 characters.
- The constraints on local backup paths are as follows:
 - Local backup is supported only in Linux.
 - The local backup path must be valid, or web tamper protection will not take effect.
 - The local backup path cannot overlap with the added protected directory.
 - The available capacity of the disk where the local backup path is located is greater than the size of all protected directories.

Adding a Protected Directory

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Web Tamper Protection**, click **Configure Protection**.

Step 4 Click **Settings** under **Protected Directory Settings**.

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 6-9](#).

Table 6-9 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.
Excluded Subdirectory	<ul style="list-style-type: none">– Subdirectories that do not need to be protected in the protected directory, such as temporary file directories.– Separate subdirectories with semicolons (;). A maximum of 10 subdirectories can be added.	The subdirectory is a relative directory in the protected directory.

Parameter	Description	Restriction
Excluded File Types	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Only Linux is supported. - 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.

Parameter	Description	Restriction
Excluded File Path	<ul style="list-style-type: none">– Paths that do not need to be protected in the protected directory.– Separate multiple paths with semicolons (;). A maximum of 50 paths can be added. The maximum length of a path is 256 characters.– A single path cannot start with a space or end with a slash (/).	The excluded file path is the relative file path of the 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 [Managing Remote Backup Servers](#).

1. On the **Protected Directory Settings** page, click **Enable Remote Backup**.
2. Select a backup server from the drop-down list box.
3. Click **OK**.

----End

Follow-Up Procedure

- Export a protected directory: If you have configured a large number of protected directories, you can click  on the protected directory configuration page to export the configurations of all protected directories to your local PC.
- Suspend protection: You can suspend WTP for a directory if needed. It is recommended 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.

6.2.2 Managing Remote Backup Servers

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.

Constraints

Only the servers that are protected by the HSS WTP edition support the operations described in this section.

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.

Adding a Remote Backup Server


- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** Choose **Prevention > Web Tamper Protection**, click **Configure Protection**.
- Step 4** Click **Settings** under **Protected Directory Settings**.
- Step 5** Click **Manage Remote Backup**. In the dialog box that is displayed, click **Add Backup Server**. For details, see [Table 6-10](#).

Table 6-10 Backup server parameters


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.
Backup Path	<p>Path of remote backup files.</p> <ul style="list-style-type: none">If the protected directories of multiple servers are backed up to the same remote backup server, the data will be stored in separate folders named after agent IDs. Assume the protected directories of the two servers are /hss01 and hss02, and the agent IDs of the two servers are f1fdbabc-6cdc-43af-acab-e4e6f086625f and f2ddbabc-6cdc-43af-abcd-e4e6f086626f, and the remote backup path is /hss01. The corresponding backup paths are /hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f and /hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f.If WTP is enabled for the remote backup server, do not set the remote backup path to any directories protected by WTP. Otherwise, remote backup will fail.

Step 6 Click **OK**.

----End

Enabling remote backup

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Web Tamper Protection**, click **Configure Protection**.

Step 4 Click **Settings** under **Protected Directory Settings**.

Step 5 Click **Enable Remote Backup** and select a remote backup server.

Step 6 Click **OK** to start remote backup.

----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.

6.2.3 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.

Constraints


Only the servers that are protected by the HSS WTP edition support the operations described in this section.

Rules for Setting an Unprotected Period

- Unprotected period \geq 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.

Procedure

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Web Tamper Protection**, click **Configure Protection**.

Step 4 On the **Configure Protection** tab, click **Settings** under **Scheduled Protection**.

Step 5 Set the unprotected period and days in a week to automatically disable protection.

1. Click **Add Unprotected Period**. Configure parameters in the dialog box that is displayed.

NOTE

Configuration constraints:


- Unprotected period \geq 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.

2. Click **OK**.

3. Select the days to disable protection.

For example, if you select **Mon.**, **Thu.**, and **Sat.**, the server automatically disables the WTP function during the unprotected period on these days.

4. Click **OK**.

Step 6 Return to the **Configure Protection** tab and toggle on  to enable **Scheduled Protection**.

----End

6.2.4 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.

Constraints


Only the servers that are protected by the HSS WTP edition support the operations described in this section.

Prerequisites


- You are using a server running the Linux OS.
- Dynamic web tamper protection is provided only for Tomcat of JDK 8.

Procedure

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Web Tamper Protection**, click **Configure Protection**.

Step 4 On the **Configure Protection** tab, toggle on  to enable **Dynamic WTP**.

Step 5 In the displayed dialog box, modify the **Tomcat bin Directory**.

To enable dynamic WTP, you need to modify the Tomcat bin directory first. The system presets the **setenv.sh** script in the bin directory for setting anti-tamper program startup parameters. After enabling dynamic WTP, restart Tomcat to make this setting take effect.

Step 6 Click **OK** to enable dynamic WTP.

----End

6.2.5 Viewing WTP Reports

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


Constraints

Only the servers that are protected by the HSS WTP edition support the operations described in this section.

Prerequisites

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, click , select a region, and choose **Security > Host Security Service**.
 - Step 3** Choose **Prevention > Web Tamper Protection** and click the **Servers** tab. Locate the row that contains the target server, and click **View Report** in the **Operation** column.
 - Step 4** View details on the report page.
- End

6.2.6 Viewing WTP Events

Once static WTP is enabled, the HSS service will comprehensively check protected directories you specified. You can check records about detected tampering of host protection files.


Constraints

Only the servers that are protected by the HSS WTP edition support the operations described in this section.

Prerequisites

- **Agent Status** of the server is **Online**, and its **WTP Status** is **Enabled**.
- Static WTP is enabled.

Procedure

- Step 1** Log in to the management console.
 - Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
 - Step 3** Choose **Prevention > Web Tamper Protection** and click **Events** to view the tampering records of protected files on servers.
- End

6.2.7 Adding a Privileged Process

If WTP is enabled, the content in the protected directories is read-only. To allow certain processes to modify files in the directories, 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.

Constraints


- Only the servers that are protected by the HSS WTP edition support the operations described in this section.
- For Linux systems, only x86 OSs with kernel 4.18 support this function.
- The privileged process takes effect only for Agent 3.2.4 or later.
- A maximum of 10 privileged processes can be added to each server.

Prerequisites

The **Protection Status** of the server must be **Protected**. To view the status, choose **Prevention > Web Tamper Protection**. Click the **Servers** tab.

Adding a Privileged Process

Step 1 Log in to the management console.

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

Step 3 Choose **Prevention > Web Tamper Protection**, click **Configure Protection**.

Step 4 Click **Privileged Process Settings** and then **Settings**.

Step 5 On the **Privileged Process Settings** page, click **Add Privileged Process**.

Step 6 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 7 Click **OK**.

Step 8 Enable **Trust Subprocess** to trust the subprocess in the path of the added privileged file.

NOTE

When this function is enabled, subprocesses at the five levels under all privileged process files are trusted.

----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 privileged processes should be deleted in a timely manner as they may be exploited by attackers.

6.3 Ransomware Prevention

6.3.1 Purchasing a Backup Vault

Scenario

After enabling ransomware protection, you need to configure a backup vault to periodically back up your servers, minimizing the loss caused by ransomware.

If you have not purchased a server backup vault, you cannot enable ransomware protection for your servers. If you have purchased a server backup vault, you can [enable ransomware protection](#) for your servers.

Purchasing a Backup Vault


- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** Choose **Prevention > Ransomware Prevention**.
- Step 4** Click the **Protected Servers** tab and click **Buy Server Backup Vault**.
- Step 5** In the dialog box that is displayed, set the vault parameters. For details about the parameters, see [Parameters for purchasing backup capacity](#).

Table 6-11 Parameters for purchasing backup capacity

Parameter	Description
Billing Mode	Select Yearly/Monthly or On-demand as required. <ul style="list-style-type: none">• Yearly/Monthly: You are billed based on the purchase period specified in the order.• On-demand: You pay for the duration you use the resources. Prices are calculated by hour, and no minimum fee is required.
Region	Region of the backup vault you want to purchase
Capacity	Select the size of the backup vault as required.
Required Duration	Select the required duration if you selected Yearly/Monthly for Billing Mode .

Parameter	Description
Price	<ul style="list-style-type: none">• Yearly/Monthly: You are billed based on the storage capacity and available duration you purchased.• On-demand: You are billed based on the storage capacity you used.

Step 6 Click **OK**.

- If **Yearly/Monthly** is selected:
 - a. The order confirmation page is displayed.
 - b. Confirm the order and click **Pay**.
- If **On-demand** is selected:

The capacity is successfully purchased.

 **NOTE**

The backup vault will be charged after the ransomware protection is enabled. Ensure that your account balance is sufficient.

----End

6.3.2 Enabling Ransomware Prevention

Prerequisites


- You have enabled HSS premium, WTP, or container edition.
- You have purchased a backup vault. For details, see [Purchasing a Backup Vault](#). If you have not purchased a backup vault, the **Add Server** button is unavailable.

Constraints

- Only premium, WTP, and container editions support ransomware protection.


Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prevention > Ransomware Prevention**. Click the **Protected Servers** tab. Click **Add Server**.

Step 4 In the dialog box that is displayed, select the target system to be protected and configure a protection policy.

- **OS:** Select the server system to be protected.
- **Ransomware Prevention:** Enable or disable ransomware prevention.
 - Enable: 


- Disable: 
- **Policy:** Select an existing policy or create a protection policy.
- **Use policy:** Select an existing protection policy. For details, see [Parameters for selecting an existing policy](#).

Table 6-12 Parameters for selecting an existing policy

Parameter	Description
Policy	Select an existing policy.
Action	Select a ransomware event processing mode supported by the selected protection policy. <ul style="list-style-type: none"> ▪ Report alarm and isolate ▪ Report alarm
Honeypot Protection	After honeypot protection is enabled, the system deploys honeypot files in protected directories and key directories (unless otherwise specified by users). A honeypot file occupies only a few resources and does not affect your server performance. If ransomware prevention is enabled, this function is enabled by default. NOTE Currently, Linux servers support dynamic generation and deployment of honeypot files. Windows servers support only static deployment of honeypot files.

- Create new: Create a protection policy on the current page. For details about the parameters, see [Parameters for creating a protection policy](#).

Table 6-13 Protection policy parameters

Parameter	Description	Example Value
Policy	Policy name	test
Action	Indicates how an event is handled. <ul style="list-style-type: none"> ▪ Report alarm and isolate ▪ Report alarm 	Report alarm and isolate

Parameter	Description	Example Value
HoneyPot Protection	<p>After honeypot protection is enabled, the system deploys honeypot files in protected directories and key directories (unless otherwise specified by users). A honeypot file occupies only a few resources and does not affect your server performance.</p> <p>If ransomware prevention is enabled, this function is enabled by default.</p> <p>NOTE Currently, Linux servers support dynamic generation and deployment of honeypot files. Windows servers support only static deployment of honeypot files.</p>	Enabled
HoneyPot File Directories	<p>Protected directories (excluding subdirectories).</p> <p>Separate multiple directories with semicolons (;). You can configure up to 20 directories.</p> <p>This parameter is mandatory for Linux servers and optional for Windows servers.</p>	<p>Linux: /etc/lesuo</p> <p>Windows: C:\Test</p>
Excluded Directory (Optional)	<p>Directories where honeypot files are not deployed.</p> <p>Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.</p>	<p>Linux: /test</p> <p>Windows: C:\ProData</p>
Protected File Type	<p>Types of files to be protected.</p> <p>More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups.</p> <p>This parameter is mandatory for Linux servers only.</p>	Select all

Parameter	Description	Example Value
(Optional) Process Whitelist	Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms. This parameter is mandatory only for Windows servers.	-

Step 5 After the configuration is complete, click **Next** to configure the vault.

 **NOTE**

Server backup must be enabled.

Select the target vault. For details about the vault list, see [Table 6-14](#).

 **NOTE**

When selecting a vault, you are advised to determine the required capacity based on the backup rules, retention period, and server asset size. Select a vault with enough available capacity. Otherwise, the backup may fail.

Table 6-14 Vault list parameters


Parameter	Description
Vault Name	Name of the target vault
Vault ID	ID of the target vault
Vault Status	Status of the target vault. <ul style="list-style-type: none"> • Available • Frozen
Used/Total Vault Capacity (GB)	Current usage and total capacity of the target vault


Parameter	Description
Used Capacity (GB)	<p>Total capacity of the server bound to the target vault.</p> <p>For example:</p> <p>Three servers with 60 GB hard disks are bound to vault A with 200 GB capacity.</p> <ul style="list-style-type: none"> The used capacity is the total storage capacity of the servers bound to vault A (3 x 60 GB = 180 GB). The used capacity does not occupy the capacity of vault A. The used capacity indicates the maximum capacity required for backing up servers bound to vault A. The used capacity cannot be greater than the capacity of vault A. Otherwise, the backup may fail.
Number Bound Servers	Number of servers associated with the target vault
Backup Policy Status	Status of the rule for automatically backing up server data in the target vault

Step 6 Click **Next** and select servers. You can search for a server by its name or by filtering.

Step 7 Confirm the information and click **OK** to return to the protected server list.

Step 8 In the list of protected servers, check the **Backup Policy Status** of the server for which ransomware protection has been enabled.

- **Enabled:** Server backup is enabled. The vault automatically backs up servers based on the associated backup policy.
- **Unbound:** Server backup is disabled. The vault is not associated with a backup policy. Perform the following steps to associate a backup policy with the vault:
 - Record the name or ID of the vault that is not associated with any backup policy.
 - Move the cursor to  in the **Backup Policy Status** column of the server, and click **CBR**.
 - In the navigation tree on the left, choose **Policies**.
 - On the displayed page, click **Create Policy** to create a backup policy.
For details, see "Creating a Backup Policy" in *Cloud Backup and Recovery User Guide*.
 - In the navigation tree on the left, choose **Cloud Server Backups**.
 - On the **Vaults** tab page, locate the vault ID you recorded in step **Step 8.a**.

- g. Locate the row that contains the target vault, click **Apply Backup Policy** in the **Policy Status** column, select a backup policy, and click **OK**.
- h. In the upper left corner of the page, click  and choose **Security** > HSS to go to the HSS page.
- i. In the navigation pane, choose **Prevention** > **Ransomware Prevention**. Click the **Protected Servers** tab. The **Backup Policy Status** of the server for which ransomware protection has been enabled is **Enabled**.

Step 9 If the ransomware protection status of the target server is **Enabled** and the backup policy status of the vault is **Enabled**, ransomware protection is successfully enabled for the server.

----End

6.3.3 Preventing Ransomware

Prerequisites


You have enabled HSS premium, WTP, or container edition.

Constraints

- After ransomware protection is enabled, you need to handle ransomware alarms and fix the vulnerabilities in your systems and middleware in a timely manner.

Checking the Ransomware Prevention Overview

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prevention** > **Ransomware Prevention**. Check ransomware prevention details.

Table 6-15 Ransomware prevention parameters

Parameter		Description	Example Value
Time range		Select a time range to check ransomware defense statistics. Valid values: Last 24 hours, Last 3 days, Last 7 days, Last 30 days	Last 30 days
Protection Statistics	Protected Servers	Number of servers protected against ransomware.	-
	Events	Number of ransomware-related events detected within the specified time range.	-

Parameter		Description	Example Value
Back up Statistics	Backed Up Servers	Number of servers whose data has been backed up.	-
	Backup and Restoration Tasks	Number of server data restoration tasks. You can click the number to view the task progress.	-
Protected Servers	Server Name/ID	Server name and ID. You can click a server name to view its details.	-
	IP Address	EIP and private IP address of a server.	-
	OS	Server OS.	Linux
	Server Status	Server status. It can be: <ul style="list-style-type: none"> ● Running ● Stopped 	-
	Ransomware Protection Status	Ransomware protection status of a server. Its value can be: <ul style="list-style-type: none"> ● Enabling ● Enabled ● Disabling ● Disabled 	Enabled
	Policy	Policy used for the server.	-
	Events	Number of events detected within the selected time range.	-
	Backup	Status of the backup function. Its value can be: <ul style="list-style-type: none"> ● Enabled: Automatic full data backup has been enabled for a server. ● Disabled: Automatic full data backup is disabled for a server. 	Enabled
	Backup Policy Status	Status of the backup policy associated with the target server	Enabled
	Vault Status	Status of the vault associated with the backup on the target server	Available
Associated Vault	Name of the vault bound to the target server	-	

Parameter		Description	Example Value
	Bound Servers	Number of servers associated with the backup vault	3
	Used/ Total Vault Capacity (GB)	The used capacity and total capacity of the vault associated with the target server	30/400
	Backups	Number of backups generated in the vault	18
Policies	Policy	Policy name.	-
	Action	Action of a policy. Its value can be: <ul style="list-style-type: none"> ● Report alarm: If a virus is detected, an alarm will be reported. ● Report alarm and isolate: If a virus is detected, an alarm will be reported and the virus will be isolated. 	Report alarm and isolate
	Honeypot Protection	Files and directories that store invalid data on servers and are used as honeypots. If ransomware prevention is enabled, this function is enabled by default. After honeypot protection is enabled, the system deploys honeypot files in protected directories and key directories (unless otherwise specified by users). A honeypot file occupies only a few resources and does not affect your server performance.	Enabled
	Run-time Detection	Status of runtime detection of a policy. The value can be: <ul style="list-style-type: none"> ● Enabled ● Disabled 	Disabled
	OS	OS of the server to which the target policy is bound.	Windows
	Associated Servers	Number of servers associated with the policy.	-

----End

Viewing Backup and Restoration Tasks

NOTICE

The backup of HSS ransomware protection depends on Cloud Backup and Recovery (CBR). Before enabling server backup, ensure that you have applied for CBR.

- Step 1** Log in to the management console and go to the HSS page.
- Step 2** In the navigation pane, choose **Prevention > Ransomware Prevention**. Click the number of backup and restoration tasks.
- Step 3** In the dialog box that is displayed, view the backup and restoration task details. You can filter or search for a server by its name or status. For more information, see [Table 6-16](#).

Table 6-16 Backup and restoration task parameters

Parameter	Description	Example Value
Server Name/ID	Name or ID of a server that executes a restoration task.	-
Backup Name	Name of a backup file.	-
Restoration Status	Restoration status of a server. It can be: <ul style="list-style-type: none">● Succeeded● Skipped● Failed● In progress● Timed out● Waiting If a task was skipped, failed, or timed out, perform restoration again.	Succeeded
Start/End Time	Start and end time of backup and restoration.	-

----End

Restoring Server Data

NOTICE

The backup of HSS ransomware protection depends on Cloud Backup and Recovery (CBR). Before enabling server backup, ensure that you have applied for CBR.

- Step 1** Log in to the management console and go to the HSS page.
- Step 2** In the navigation pane, choose **Prevention > Ransomware Prevention**. Click the **Protected Servers** tab. In the **Operation** column of the target server, click **More > Restore Data**.
- Step 3** In the dialog box that is displayed, view information about the server to be restored. You can search for the backup data source to be restored by filtering the backup status and searching for the backup name. For more information, see [Table 6-17](#).

Table 6-17 Backup data source parameters

Parameter	Description	Example Value
Backup Name	Name of a backup file.	-
Backup Status	Backup status. It can be: <ul style="list-style-type: none">• Available• Creating• Deleting• Restoring• Error A backup in Available state can be used for restoration.	Available
Purpose	Backup purpose. It can be: <ul style="list-style-type: none">• Periodic execution: Data is backed up based on the backup period configured in the backup policy.• Ransomware protection: Data is backed up immediately when a server is attacked by ransomware.	Periodic execution
Execution Time	Time when the data source was backed up.	-

- Step 4** In the **Operation** column of a backup, click **Restore Data**.

NOTE

Only a backup in the available state can be restored.

Step 5 In the dialog box that is displayed, confirm the server information and click **OK**.

----End

Increasing the Backup Capacity

NOTICE

The backup of HSS ransomware protection depends on Cloud Backup and Recovery (CBR). Before enabling server backup, ensure that you have applied for CBR.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Prevention > Ransomware Prevention**. The protected server list is displayed. Click **Add Capacity** in the **Operation** column of the target server.

Step 3 In the dialog box that is displayed, configure the capacity.

Step 4 If the information is correct, click **OK**. The payment page is displayed. After the payment is complete, return to the **Protected Server** tab page to view the storage capacity of the target server.

- If the payment is not complete, the **Vault Status** of the target server displays **Locked**. After the payment, the status becomes normal.

----End

Modifying a Backup Policy

NOTICE

The backup of HSS ransomware protection depends on Cloud Backup and Recovery (CBR). Before enabling server backup, ensure that you have applied for CBR.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Prevention > Ransomware Prevention**. The protected server list is displayed. Click the policy name in the **Backup Policy Status** column of the target server.

Step 3 Configure the policy in the dialog box that is displayed. For more information, see [Table 6-18](#).

Table 6-18 Policy parameters

Parameter	Description	Example Value
Backup Frequency	Data can be automatically backed up on specific days in a week, or at a fixed interval. <ul style="list-style-type: none"> Weekly: Select one or more days in a week to back up data. Day based: The range of the backup interval is 1 to 30 days. 	Weekly
Execution Time	Time when automated backup is started. NOTE Example of policy configurations Policy 1: Set Backup Frequency to Weekly , select Wednesday and Saturday , and set Execution Time to 00:00 and 13:00 . Data will be automatically backed up at 00:00 and 13:00 every Wednesday and Saturday. Policy 2: Set Backup Frequency to Day based and set the interval to two days. Set Execution Time to 02:00 and 14:00 . Data will be automatically backed up at 02:00 and 14:00 at an interval of two days.	00:00, 07:00
Timezone	Select the time zone of the backup time.	UTC+08:00

Step 4 Confirm the settings and click **Next**. Configure the backup retention rule.

- Type: Backup Quantity**

Configure the backup policy. For more information, see [Table 6-19](#).

Table 6-19 Parameters for data retention by quantity

Parameter	Description	Example Value
Rule	Number of latest backups to be retained. NOTICE This setting takes effect no matter how you configure advanced options. For example, if the rule is configured to keep the most recent 30 backups, and Advanced Options are configured to keep the latest backup in the last 3 months (90 days), the latest 30 backups will be retained.	30

Parameter	Description	Example Value
(Optional) Advanced Options	<p>You can retain the latest backup in a day, a week, a month, or a year.</p> <ul style="list-style-type: none"> - Daily backup: The latest backup on each of the specified days is retained. - Weekly backup: The latest backup on each day of the specified weeks is retained. - Monthly backup: The latest backup on each day of the specified months is retained. - Yearly backup: The latest backup on each day of the specified years is retained. <p>NOTE If multiple rules are configured, the rule with the longest retention period takes effect.</p>	Keep the most recent backup from each of the last three months

- **Type: Time period**

Configure the backup policy. For more information, see [Table 6-20](#).

Table 6-20 Parameters for data retention by time period

Parameter	Description	Example Value
Rule	<p>Select or customize a backup retention period. The system will automatically retain backups and delete old ones based on your settings. The retention period can be:</p> <ul style="list-style-type: none"> - Days - 1 month - 3 months - 6 months - 1 year 	3 months

- **Type: Permanent**

Backup data will be permanently stored.

 **NOTE**

If the **Retention Type** of a rule is changed from **Time period** to Permanent, historical backups will still be deleted by following based on the **Time period** settings.

Step 5 Click **OK**.

----End


6.3.4 Disabling Ransomware Prevention

Scenario

You can disable ransomware protection as needed. After protection is disabled, your server may be intruded by ransomware. Exercise caution when performing this operation.

Disabling Ransomware Prevention

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prevention > Ransomware Prevention**. Click the **Protected Servers** tab.

Step 4 Click **More > Disable Protection** in the **Operation** column of the target server.

Step 5 Confirm the information and click **OK**.

----End

Follow-up Operations

Disabling ransomware prevention does not stop data backup. If you no longer need backup, dissociate your servers from CBR by referring to "Dissociating a Resource" in Cloud Backup and Recovery User Guide. If you no longer need a backup vault, you can delete it by referring to "Deleting a Vault" in Cloud Backup and Recovery User Guide.

6.3.5 Managing Protection Policies

NOTICE


Currently, you can create a ransomware prevention policy only when enabling ransomware prevention.

Constraints

Only premium, WTP, and container editions support ransomware protection.

Creating a Policy

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prevention > Ransomware Prevention**. Click the **Protected Servers** tab. Click **Add Server**.

Step 4 In the slide pane that is displayed, select **Linux**, enable protection, and select **Create new**. For more information, see [Table 6-21](#).

The following uses a Linux server as an example.

Table 6-21 Protection policy parameters

Parameter	Description	Example Value
Policy	Policy name	test
Action	Indicates how an event is handled. <ul style="list-style-type: none">• Report alarm and isolate• Report alarm	Report alarm and isolate
Honeypot Protection	After honeypot protection is enabled, the system deploys honeypot files in protected directories and key directories (unless otherwise specified by users). A honeypot file occupies only a few resources and does not affect your server performance. If ransomware prevention is enabled, this function is enabled by default. NOTE Currently, Linux servers support dynamic generation and deployment of honeypot files. Windows servers support only static deployment of honeypot files.	Enabled
Honeypot File Directories	Protected directories (excluding subdirectories). Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	Linux: /etc/lesuo Windows: C:\Test
Excluded Directory (Optional)	Directories where honeypot files are not deployed. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	Linux: /test Windows: C:\ProData

Parameter	Description	Example Value
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. This parameter is mandatory for Linux servers only.	Select all
(Optional) Process Whitelist	Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms. This parameter is mandatory only for Windows servers.	-

Step 5 Click **Next** and select servers. You can search for a server by its name or by filtering.

Step 6 Click **OK** to enable ransomware protection and create the policy.

Step 7 In the navigation pane, choose **Prevention > Ransomware Prevention**. Click the **Policies** tab and check the new policy.

----End

Modifying a Policy

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane, choose **Prevention > Ransomware Prevention**. Click the **Policies** tab.

Step 3 Click **Edit** in the **Operation** column of a policy. Edit the policy configurations and associated servers. For more information, see [Protection policy parameters](#).

The following uses a Linux server as an example.

Table 6-22 Protection policy parameters

Parameter	Description	Example Value
Policy	Policy name	test
Action	Indicates how an event is handled. <ul style="list-style-type: none"> Report alarm and isolate Report alarm 	Report alarm and isolate

Parameter	Description	Example Value
HoneyPot Protection	<p>After honeyPot protection is enabled, the system deploys honeyPot files in protected directories and key directories (unless otherwise specified by users). A honeyPot file occupies only a few resources and does not affect your server performance.</p> <p>If ransomware prevention is enabled, this function is enabled by default.</p> <p>NOTE Currently, Linux servers support dynamic generation and deployment of honeyPot files. Windows servers support only static deployment of honeyPot files.</p>	Enabled
HoneyPot File Directories	<p>Protected directories (excluding subdirectories).</p> <p>Separate multiple directories with semicolons (;). You can configure up to 20 directories.</p> <p>This parameter is mandatory for Linux servers and optional for Windows servers.</p>	Linux: /etc/lesuo Windows: C:\Test
Excluded Directory (Optional)	<p>Directories where honeyPot files are not deployed.</p> <p>Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.</p>	Linux: /test Windows: C:\ProData
Protected File Type	<p>Types of files to be protected.</p> <p>More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups.</p> <p>This parameter is mandatory for Linux servers only.</p>	Select all
(Optional) Process Whitelist	<p>Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms.</p> <p>This parameter is mandatory only for Windows servers.</p>	-

Step 4 Confirm the policy information and click **OK**.

----End

Deleting a Policy

- Step 1** Log in to the management console and go to the HSS page.
- Step 2** In the navigation pane, choose **Prevention > Ransomware Prevention**. Click the **Policies** tab.
- Step 3** Click **Delete** in the **Operation** column of the target policy.

 **NOTE**

After a policy is deleted, the associated servers are no longer protected. Before deleting a policy, you are advised to bind its associated servers to other policies.

- Step 4** Confirm the policy information and click **OK**.

----End

6.4 File Integrity Monitoring


You can check the statistics and details about file changes on your servers, including affected servers, file types, paths, and content.

6.4.1 Viewing File Integrity Management

Constraints

The premium and higher editions support operations related to file integrity.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security > Host Security Service**.
- Step 3** Choose **Prevention > File Integrity Monitoring**. On the displayed file management page, check its servers and modified files.


----End

6.4.2 Checking Change Details

Constraints

The premium and higher editions support operations related to file integrity.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.

Step 3 Choose **Prevention > File Integrity Monitoring**. The **Server** tab will be displayed.

Step 4 Click a server name to go its change details page.

Table 6-23 Parameters about file changes

Parameter	Description	Example Value
File Name	Name of a modified file.	du
Path	Path of a modified file.	-
Change Description	Description of the change. To view the change details, hover the cursor over the change content.	SHA2560ba0c4b5e48e55a6 is changed to 4f6079f5b37d1513 .
Server Name	Name of the server where the change is detected.	-
Type	Type of a modified file. Its value can be: <ul style="list-style-type: none">• File	File
Action	How a file was modified. <ul style="list-style-type: none">• Create• Modify• Delete	Modify
Time Range	Time when a file was modified.	-

----End


6.4.3 Checking Modified Files

Constraints

The premium and higher editions support operations related to file integrity.

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Prevention > File Integrity Monitoring**. Click the **Monitored Files** tab. For details about parameters, see [Table 6-23](#) in [Checking Change Details](#).

----End

7 Intrusion Detection

7.1 Alarms

7.1.1 HSS Alarms

7.1.1.1 Server Alarms

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

 **NOTE**

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

Constraints

Servers that are not protected by HSS do not support alarm-related operations.

Supported Alarms and Events

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WT Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
Malware	Unclassified malware	<p>Malicious programs include Trojans and web shells implanted by hackers to steal your data or control your servers.</p> <p>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.</p> <p>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.</p>	√	√	√	Linux and Windows	√	√
	Viruses	Detect viruses in server assets, report alarms, and support automatic or manual viruses isolation and killing based on the alarms.	√	√	√	Linux and Windows	√	√
	Worms	Detect and kill worms on servers and report alarms.	√	√	√	Linux and Windows	√	√
	Trojans	Detect and remove Trojan and viruses on servers and report alarms.	√	√	√	Linux and Windows	√	√

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WT P Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
	Botnets	Detect and kill botnets on servers and report alarms.	√	√	√	Linux and Windows	√	√
	Backdoors	Detect backdoors in servers and reports alarms.	√	√	√	Linux and Windows	√	√
	Rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders.	√	√	√	Linux	√	×
	Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.	×	√	√	Linux and Windows	√	√ (Partially supported)
	Hacker tools	Detect and kill hacker tools on servers and reports alarms.	√	√	√	Linux and Windows	√	√

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WT P Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
	Web shells	Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. You can configure the web shell detection rule in the Web Shell Detection rule on the Policies page. HSS will check for suspicious or remotely executed commands. You need to add a protected directory in policy management. For details, see Web Shell Detection .	√	√	√	Linux and Windows	√	×
	Mining	Detect, scan, and remove mining software on servers, and report alarms.	√	√	√	Linux and Windows	√	√
Vulnerability Exploits	Remote code execution	Detect and report alarms on server intrusions that exploit vulnerabilities in real time.	√	√	√	Linux and Windows	√	×
	Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms.	√	√	√	Linux	√	×

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WT Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
	Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms.	√	√	√	Linux	√	×
	MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms.	√	√	√	Linux	√	×
Abnormal System Behavior	Reverse shells	<p>Monitor user process behaviors in real time to detect reverse shells caused by invalid connections.</p> <p>Reverse shells can be detected for protocols including TCP, UDP, and ICMP.</p> <p>You can configure the reverse shell detection rule in the Malicious File Detection rule on the Policies page. HSS will check for suspicious or remotely executed commands.</p>	√	√	√	Linux	√	×

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WT P Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
	File privilege escalations	Detect file privilege escalation behaviors and generate alarms.	√	√	√	Linux	√	×
	Process privilege escalations	Detect the privilege escalation operations of the following processes and generate alarms: <ul style="list-style-type: none"> • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities 	√	√	√	Linux	√	×
	Important file changes	Monitor important system files (such as ls, ps, login, and top) in real time and generate alarms if these files are modified. For details about the monitored paths, see Monitored Important File Paths . HSS reports all the changes on important files, regardless of whether the changes are performed manually or by processes.	√	√	√	Linux	√	×

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
	File/Directory changes	Monitor system files and directories in real time and generate alarms if such files are created, deleted, moved, or if their attributes or content are modified.	√	√	√	Linux and Windows	√	×
	Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: <ul style="list-style-type: none"> Abnormal CPU usage Processes accessing malicious IP addresses Abnormal increase in concurrent process connections 	√	√	√	Linux and Windows	√	× (Partially supported)
	High-risk commands and executions	You can configure what commands will trigger alarms in the High-risk Command Scan rule on the Policies page. HSS checks executed commands in real time and generates alarms if high-risk commands are detected.	√	√	√	Linux and Windows	√	×

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WT P Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
	Abnormal shells	<p>Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files.</p> <p>You can configure the abnormal shell detection rule in the Malicious File Detection rule on the Policies page. HSS will check for suspicious or remotely executed commands.</p>	√	√	√	Linux	√	×
	Suspicious cron tasks	<p>Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders.</p> <p>You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans.</p>	×	√	√	Linux and Windows	√	×
	System protection disabling	Detect the preparations for ransomware encryption: Disable the Windows defender real-time protection function through the registry. Once the function is disabled, an alarm is reported immediately.	√	√	√	Windows	√	×
	Backup deletion	Detect the preparations for ransomware encryption: Delete backup files or files in the Backup folder. Once backup deletion is detected, an alarm is reported immediately.	√	√	√	Windows	√	×

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
	Suspicious registry operations	Detect operations such as disabling the system firewall through the registry and using the ransomware Stop to modify the registry and write specific strings in the registry. An alarm is reported immediately when such operations are detected.	√	√	√	Windows	√	×
	System log deletions	An alarm is generated when a command or tool is used to clear system logs.	√	√	√	Windows	√	×
	Suspicious command executions	<ul style="list-style-type: none"> Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. Detect suspicious remote command execution. 	√	√	√	Windows	√	×

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WTP Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
Abnormal User Behavior	Brute-force attacks	<p>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.</p> <p>Detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts.</p> <ul style="list-style-type: none"> If the number of brute-force attacks (consecutive incorrect password attempts) from an IP address reaches 5 within 30 seconds, the IP address will be blocked. <p>By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours.</p> <ul style="list-style-type: none"> 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. 	√	√	√	Linux and Windows	√	×

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WT P Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
	Abnormal logins	<p>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.</p> <ul style="list-style-type: none"> Check and handle remote logins. You can check the blocked login IP addresses, and who used them to log in to which server at what time. If a user's login location is not any common login location, an alarm will be triggered. Trigger an alarm if a user logs in by a brute-force attack. 	√	√	√	Linux and Windows	√	×
	Invalid accounts	<p>Hackers can probably crack unsafe accounts on your servers and control the servers.</p> <p>HSS checks suspicious hidden accounts and cloned accounts and generates alarms on them.</p>	√	√	√	Linux and Windows	√	×
	User account added	Detect the commands used to create hidden accounts. Hidden accounts cannot be found in the user interaction interface or be queried by commands.	√	√	√	Windows	√	×
	Password theft	Detect the abnormal obtaining of system accounts and password hashes on servers and report alarms.	√	√	√	Windows	√	×

Event Type	Alarm Name	Description	Enterprise Edition	Premium Edition	WT P Edition	Supported OS	Add to Alarm Whitelist	Isolate and Kill
Abnormal Network Access	Suspicious download request	An alarm is generated when a suspicious HTTP request that uses system tools to download programs is detected.	√	√	√	Windows	√	×
	Suspicious HTTP requests	An alarm is generated when a suspicious HTTP request that uses a system tool or process to execute a remote hosting script is detected.	√	√	√	Windows	√	×
Report anomalies	Port scan	Detect scanning or sniffing on specified ports and report alarms.	×	√	√	Linux	×	×
	Host scan	Detect the network scan activities based on server rules (including ICMP, ARP, and nbtscan) and report alarms.	×	√	√	Linux	√	×

Monitored Important File Paths

Type	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

7.1.1.2 Viewing Intrusion Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of 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. You can manually handle the alarmed items.

The status of a handled event changes from **Unhandled** to **Handled**.

NOTE

Alarms generated by AV detection and HIPS detection are displayed under different types of events.

- Alarms generated by AV detection are displayed only under the **Malware** events.
- Alarms generated by HIPS detection are displayed in subcategories of all events.

Constraints 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. For details, see [Viewing a Policy Group](#).
- Other detection items cannot be manually disabled.
- Servers that are not protected by HSS do not support operations related to alarms and events.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security** > Host Security Service.
- Step 3** In the navigation pane on the left, choose **Detection** > **Alarms** and click **Server Alarms**.

Table 7-1 Alarm statistics

Parameter	Description
Time range	You can select a fixed period or customize a time range to search for alarms. Only alarms generated within 30 days can be queried. The options are as follows: <ul style="list-style-type: none">• Last 24 hours• Last 3 days• Last 7 days• Last 30 days
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.
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. The blocked IP address list displays the server name, attack source IP address, login type, blocking status, number of blocks, blocking start time, and the latest blocking time. If a valid IP address is blocked by mistake (for example, after O&M personnel enter incorrect passwords for multiple times), you can manually unblock it. If a server is frequently attacked, you are advised to fix its vulnerabilities in a timely manner and eliminate risks. NOTICE <ul style="list-style-type: none">• After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address.• A maximum of 10,000 IP addresses can be blocked for each type of software. If your Linux server does not support ipset, a maximum of 50 IP addresses can be blocked for MySQL and vsftpd. If your Linux server does not support ipset or hosts.deny, a maximum of 50 IP addresses can be blocked for SSH.

Parameter	Description
Isolated Files	HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the Server Alarms page. You can click Isolated Files on the upper right corner to check them. You can recover isolated files. For details, see Managing Isolated Files .

Step 4 Click an alarm event in the list of event types to view the affected servers and occurrence time of the event. The following information is displayed:

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

Step 5 Click an alarm name to view its details.

----End

7.1.1.3 Managing Isolated Files

HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the **Server Alarms** page. You can click **Isolated Files** on the upper right corner to check them, and can recover isolated files anytime.


For details about events that can be isolated and killed, see [Server Alarms](#).

Constraints

Servers that are not protected by HSS do not support alarm-related operations.

Isolation and Killing Operations

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Detection** > **Alarms** and click **Server Alarms**.

Table 7-2 Alarm statistics

Parameter	Description
Time Range	<p>You can select a fixed period or customize a time range to search for alarms. Only alarms generated within 30 days can be queried.</p> <p>The options are as follows:</p> <ul style="list-style-type: none">• Last 24 hours• Last 3 days• Last 7 days• Last 30 days
Affected Servers	Number of servers for which alarms are generated.
Alarms to be Handled	<p>Number of alarms to be handled.</p> <p>By default, all unhandled alarms are displayed on the Events page.</p>
Handled Alarms	Number of handled alarms.
Blocked IP Addresses	<p>Number of blocked IP addresses. You can click the number to check blocked IP address list.</p> <p>The blocked IP address list displays the server name, attack source IP address, login type, blocking status, number of blocks, blocking start time, and the latest blocking time.</p> <p>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.</p> <p>NOTICE</p> <ul style="list-style-type: none">• After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address.• A maximum of 10,000 IP addresses can be blocked for each type of software. If your Linux server does not support ipset, a maximum of 50 IP addresses can be blocked for MySQL and vsftpd. If your Linux server does not support ipset or hosts.deny, a maximum of 50 IP addresses can be blocked for SSH.
Isolated Files	<p>HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the Server Alarms page. You can click Isolated Files on the upper right corner to check them.</p> <p>You can recover isolated files. For details, see Managing Isolated Files.</p>

Step 4 Locate an event that can be isolated and killed, click **Handle** in the **Operation** column, and select **Isolate and Kill** in the displayed box.

 NOTE

For details about events that can be isolated and killed, see [Server Alarms](#).

Step 5 Click **OK** and isolate and kill the target alarm event.

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

----End

Checking Isolated Files

Step 1 In the alarm statistics area on the **Server Alarms** page, click **View Details** under **Isolated Files** to check the isolated files.

Step 2 Check the servers, names, paths, and modification time of the 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

7.1.1.4 Handling Server Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of servers with alarms, handled alarms, unhandled alarms, blocked IP addresses, and isolated files.

The **Events** page displays the alarms generated in the last 30 days.

The status of a handled alarm changes from **Unhandled** to **Handled**.

Limitations and Constraints

- To skip the checks on high-risk command execution, privilege escalations, reverse shells, abnormal shells, or web shells, manually disable the corresponding policies in the policy groups on the **Policies** page. HSS will not check the servers associated with disabled policies. For details, see [Checking or Creating a Policy Group](#).
- Other detection items cannot be manually disabled.
- Servers that are not protected by HSS do not support operations related to alarms and events.

Procedure

This section describes how you should handle alarms to enhance server security.

NOTE

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


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security** > Host Security Service.
- Step 3** In the navigation pane on the left, choose **Detection** > **Alarms** and click **Server Alarms**.

Table 7-3 Alarm statistics

Parameter	Description
Time Range	You can select a fixed period or customize a time range to search for alarms. Only alarms generated within 30 days can be queried. The options are as follows: <ul style="list-style-type: none">• Last 24 hours• Last 3 days• Last 7 days• Last 30 days
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.
Handled Alarms	Number of handled alarms.

Parameter	Description
Blocked IP Addresses	<p>Number of blocked IP addresses. You can click the number to check blocked IP address list.</p> <p>The blocked IP address list displays the server name, attack source IP address, login type, blocking status, number of blocks, blocking start time, and the latest blocking time.</p> <p>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.</p> <p>NOTICE</p> <ul style="list-style-type: none">• After a blocked IP address is unblocked, HSS will no longer block the operations performed by the IP address.• A maximum of 10,000 IP addresses can be blocked for each type of software. If your Linux server does not support ipset, a maximum of 50 IP addresses can be blocked for MySQL and vsftpd. If your Linux server does not support ipset or hosts.deny, a maximum of 50 IP addresses can be blocked for SSH.
Isolated Files	<p>HSS can isolate detected threat files. Files that have been isolated are displayed on a slide-out panel on the Server Alarms page. You can click Isolated Files on the upper right corner to check them.</p> <p>You can recover isolated files. For details, see Managing Isolated Files.</p>

Step 4 Handle alarms.

NOTE

Alarms are displayed on the **Server Alarms** page. Here you can check up to 30 days of historical alarms.

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

- Handling all alarms
 - a. Select all of the alarms and click **hss_secAlarm_batch_operate_003**.

NOTE

Ensure that you have selected the minimum alarm event type. Otherwise, the **hss_secAlarm_batch_operate_003** button is unavailable.

- b. In the dialog box that is displayed, select a handling method, confirm the information, and click **OK**. For more information, see [Table 7-4](#).

NOTE

An alarm in the **Handled** state cannot be batch handled.

- Handling alarms in batches

- a. Select an event type, select multiple alarms, and click **Batch Handle**.
 - b. In the dialog box that is displayed, select a handling method, confirm the information, and click **OK**. For more information, see [Table 7-4](#).
- Handling a single alarm
 - a. Select an event type and click **Handle** in the **Operation** column of an alarm.
 - b. In the dialog box that is displayed, select a handling method, confirm the information, and click **OK**. For more information, see [Table 7-4](#).

Table 7-4 Alarm handling methods

Action	Description
Ignore	Ignore the current alarm. Any new alarms of the same type will still be reported by HSS.
Isolate and kill	<p>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.</p> <p>You can click Isolated Files on the upper right corner to check the files. For details, see Managing Isolated Files.</p> <p>For details about events that can be isolated and killed, see Server Alarms.</p> <p>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 ignore misreported malicious programs (if any).</p>
Mark as handled	Mark the event as handled. You can add remarks for the event to record more details.
Add to login whitelist	<p>Add false alarmed items of the Brute-force attack and Abnormal login types to the login whitelist.</p> <p>HSS will no longer report alarm on the whitelisted items. A whitelisted login event will not trigger alarms.</p> <p>The following alarms can be added to the login whitelist:</p> <ul style="list-style-type: none"> • Brute-force attacks • Abnormal logins
Add to alarm whitelist	<p>Add false alarmed items to the login whitelist.</p> <p>HSS will no longer report alarm on the whitelisted items. A whitelisted alarm will not trigger alarms.</p> <p>For details about events that can be isolated and killed, see Server Alarms.</p>

----End

7.1.2 Container Alarms

7.1.2.1 Container Alarm Events

After node protection is enabled, an agent is deployed on each container host to monitor the running status of containers in real time. The agents support escape detection, high-risk system calls, abnormal processes, abnormal files, and container environment detection. You can learn alarm events comprehensively on the **Container Alarms** page, and eliminate security risks in your assets in a timely manner.

Constraints

- Only HSS container edition supports the container security alarm function.
- Intrusion detection alarms can be generated only for Docker containers.

Container Alarm Types

Event Type	Alarm Name	Mechanism
Malware	Unclassified malware	Check malware, such as web shells, Trojan horses, mining software, worms, and other viruses and variants. The malware is found and removed by analysis on program characteristics and behaviors, AI image fingerprint algorithms, and cloud scanning and killing.
	Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion.
	Web shells	Check whether the files (often PHP and JSP files) in the web directories on containers are web shells.
Vulnerability Exploits	Vulnerability escapes	HSS reports an alarm if it detects container process behavior that matches the behavior of known vulnerabilities (such as Dirty COW, brute-force attack, runC, and shocker).
	File escapes	HSS reports an alarm if it detects that a container process accesses a key file directory (for example, /etc/shadow or /etc/crontab). Directories that meet the container directory mapping rules can also trigger such alarms.
Abnormal System Behaviors	Reverse shells	Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. You can configure the reverse shell detection rule in the Malicious File Detection rule on the Policies page. HSS will check for suspicious or remotely executed commands.

Event Type	Alarm Name	Mechanism
	Process privilege escalations	<p>After hackers intrude containers, they will try exploiting vulnerabilities to grant themselves the root permissions or add permissions for files. In this way, they can illegally create system accounts, modify account permissions, and tamper with files.</p> <p>HSS can detect the following abnormal privilege escalation operations:</p> <ul style="list-style-type: none"> • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities • File privilege escalation
	High-risk system calls	Users can run tasks in kernels by Linux system calls. CGS reports an alarm if it detects a high-risk call, such as open_by_handle_at , ptrace , setns , and reboot .
	High-risk command executions	Check executed commands in containers and generate alarms if high-risk commands are detected.
	Abnormal container processes	<ul style="list-style-type: none"> • Malicious container program HSS monitors container process behavior and process file fingerprints. It reports an alarm if it detects a process whose behavior characteristics match those of a predefined malicious program. • Abnormal processes Container services are usually simple. If you are sure that only specific processes run in a container, you can whitelist the processes on the Policy Groups page, and associate the policy with the container. HSS reports an alarm if it detects that a process not in the whitelist is running in the container.
	Sensitive file access	HSS monitors the container image files associated with file protection policies, and reports an alarm if the files are modified.

Event Type	Alarm Name	Mechanism
	Abnormal container startups	<p>HSS monitors container startups and reports an alarm if it detects that a container with too many permissions is started. This alarm does not indicate an actual attack. Attacks exploiting this risk will trigger other HSS container alarms.</p> <p>HSS container check items include:</p> <ul style="list-style-type: none"> <p>Privileged container startup (<code>privileged:true</code>) Alarms are triggered by the containers started with the maximum permissions. Settings that can trigger such alarms include the <code>-privileged=true</code> parameter in the <code>docker run</code> command, and <code>privileged: true</code> in the <code>securityContext</code> of the container in a Kubernetes pod.</p> <p>If the alarm name is Container Security Options and the alarm content contains <code>privileged:true</code>, it indicates that the container is started in privileged container mode.</p> <p>Too many container capabilities (<code>capability:[xxx]</code>) In Linux OSs, system permissions are divided into groups before assigned to containers. A container only has a limited number of permissions, and the impact scope of this container is limited in the case of an incident. However, malicious users can grant all the system permissions to a container by modifying its startup configurations.</p> <p>If the alarm name is Container Security Options and the alarm content contains <code>capabilities:[xxx]</code>, it indicates that the container is started with an overlarge capability set, which poses risks.</p> <p>Seccomp not enabled (<code>seccomp=unconfined</code>) Secure computing mode (seccomp) is a Linux kernel feature. It can restrict system calls invoked by processes to reduce the attack surface of the kernel. If <code>seccomp=unconfined</code> is configured when a container is started, system calls will not be restricted for the container.</p> <p>If the alarm name is Container Security Options and the alarm content contains <code>seccomp=unconfined</code>, it indicates that the container is started without seccomp, which poses risks.</p> <p>NOTE If seccomp is enabled, permissions will be verified for every system call. The verifications will probably affect services if system calls are frequent. Before you decide whether to enable seccomp, you are advised to test-enable it and analyze the impact on your services.</p> <p>Container privilege escalation (<code>no-new-privileges:false</code>)</p>

Event Type	Alarm Name	Mechanism
		<p>Processes can escalate permissions by running the sudo command and using SUID or SGID bits. Default container configurations do not allow privilege escalation.</p> <p>If -no-new-privileges=false is specified when a container is started, the container can escalate privileges.</p> <p>If the alarm name is Container Security Options and the alarm content contains no-new-privileges:false, it indicates that privilege escalation restriction is disabled for the container, which poses risks.</p> <ul style="list-style-type: none"> • High-risk directory mapping (mounts:[...]) For convenience purposes, when a container is started on a server, the directories of the server can be mapped to the container. In this way, services in the container can directly read and write resources on the server. However, this mapping incurs security risks. If any critical directory in the server OS is mapped to the container, improper operations in the container will probably damage the server OS. <p>HSS reports an alarm if it detects that a critical server path (/boot, /dev, /etc, /sys, and /var/run) is mounted during container startup.</p> <p>If the alarm name is Container Mount Point and the alarm content contains mounts: [{"source":"xxx","destination":"yyy"...}], it indicates that a file path mapped to the container is unsafe. In this case, check for risky directory mappings. You can configure the mount paths that are considered secure in the container information collection policy.</p> <p>NOTE Alarms will not be triggered for the files that need to be frequently accessed by Docker containers, such as /etc/hosts and /etc/resolv.conf.</p> <ul style="list-style-type: none"> • Startup of containers in the host namespace The namespace of a container must be isolated from that of a server. If a container and a server use the same namespace, the container can access and modify the content on the server, which incurs container escape risks. To prevent such problems, HSS checks the container PID, network, and whether the container namespace is host. <p>If the alarm name is Container Namespace and the alarm content contains Container PID Namespace Mode, Container IPC Namespace Mode, or Container Network Namespace Mode, it indicates that a container whose namespace is host is started.</p>

Event Type	Alarm Name	Mechanism
		In this case, check the container startup options based on the alarm information. If you are sure that the container can be trusted, you can ignore the alarm.
	Container Image blocking	If a container contains insecure images specified in the Suspicious Image Behaviors , before the container is started, an alarm will be generated for the insecure images. NOTE You need to install the Docker plug-in .
Abnormal User Behavior	Invalid accounts	Hackers can probably crack unsafe accounts on your containers and control the containers. HSS checks for suspicious hidden accounts and cloned accounts and generates alarms on them.
	Brute-force attacks	Detect and report alarms for brute-force attack behaviors, such as brute-force attack attempts and successful brute-force attacks, on containers. Detect SSH, web, and Enumdb brute-force attacks on containers. NOTE Currently, brute-force attacks can be detected only in the Docker runtime.
Abnormal Cluster Behaviors	Abnormal pod behaviors	Detect abnormal operations such as creating privileged pods, static pods, and sensitive pods in a cluster and abnormal operations performed on existing pods and report alarms.
	User information enumerations	Detect the operations of enumerating the permissions and executable operation list of cluster users and report alarms.
	Binding cluster roles	Detect operations such as binding or creating a high-privilege cluster role or service account and report alarms.
	Kubernetes event deletions	Detect the deletion of Kubernetes events and report alarms.

7.1.2.2 Viewing Container Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of containers with alarms, handled alarms, and unhandled alarms.

The **Events** page displays the alarm events generated in the last 30 days.


The status of a handled event changes from **Unhandled** to **Handled**.

Constraints

Servers that are not protected by HSS do not support operations related to alarms and events.

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Detection** > **Alarms** and click the **Container Alarms** tab to view container alarms and events.

- View the overview of container alarms and events.
 - **Alarm Statistics:** You can view the number of containers that have alarms and the number of alarms to be handled and that have been handled.
 - **Threats:** You can view the number of alarms in a container by severity.
 - **Top 5 Events:** You can view the top 5 events with the largest number of alarms in a container.
- View the container alarms of a certain type.

In the **Event Types** area, select an alarm event type to view the corresponding alarm event list. In the alarm event list, you can view the alarm threat level, alarm name, container status, pod name, and affected container name.
- View details about container alarms and events.

Click an alarm name to go to its details page. You can view the container ID, IP address, VM name, and image ID.
- View the pod details of the container alarm event.

Click the pod name of the target alarm event to view the pod details, including the node IP address, namespace, pod IP address, pod label, and container list.

----End

7.1.2.3 Handling Container Alarms

HSS displays alarm and event statistics and their summary all on one page. You can have a quick overview of alarms, including the numbers of containers with alarms, handled alarms, and unhandled alarms.

The **Events** page displays the alarms generated in the last 30 days.

The status of a handled alarm changes from **Unhandled** to **Handled**.

Constraints

Servers that are not protected by HSS do not support operations related to alarms and events.


Procedure

This section describes how you should handle alarms to enhance server security.

NOTE

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

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Detection > Alarms**, and click **Container Alarms**.

Table 7-5 Alarm statistics

Alarm Event	Description
Affected Servers	Number of containers 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.
Handled Alarms	Number of handled alarms.

Step 4 Handle alarms.

NOTE

Alarms are displayed on the **Container Alarms** page. Here you can check up to 30 days of historical alarms.

Check and handle alarms as needed. The status of a handled alarm changes from **Unhandled** to **Handled**. HSS will no longer collect its statistics.

- Handling all alarms in batches
 - a. Select an event type, select the alarms, and click **Handle All**.
 - b. In the dialog box that is displayed, select a handling method, confirm the information, and click **OK**. For more information, see [Table 7-6](#).

NOTE

An alarm in the **Handled** state cannot be batch handled.

- Handling selected alarms in batches
 - a. Select an event type, select multiple alarms, and click **Handle All**.
 - b. In the dialog box that is displayed, select a handling method, confirm the information, and click **OK**. For more information, see [Table 7-6](#).
- Handling a single alarm

- a. Select an event type, and click **Handle** in the **Operation** column of an alarm.
- b. In the dialog box that is displayed, select a handling method, confirm the information, and click **OK**. For more information, see [Table 7-6](#).

Table 7-6 Handling alarm events

Action	Description
Ignore	Ignore the current alarm. Any new alarms of the same type will still be reported by HSS.
Mark as handled	Mark the event as handled. You can add remarks for the event to record more details.

----End

7.2 Whitelist Management

7.2.1 Configuring the Login Whitelist

You can configure the IP addresses of destination servers, login IP addresses, login usernames, and user behaviors in the whitelist.

NOTE

- If the destination server IP address, login IP address, and username of a login are all whitelisted, this login will be allowed without checking.
- After an IP address is added to a whitelist by following the instructions in [Adding Login Information to the Login Whitelist](#), the alarms (if any) that have been generated for the IP address will not be automatically cleared. Handle the alarms by referring to [Viewing Intrusion Alarms](#).

You can add login information to the login whitelist in the following ways:


- Add it to the whitelist when handling false alarms of the **Brute-force attack** and **Abnormal login** types. For details, see [Viewing Intrusion Alarms](#).
- Add it to the login whitelist on the **Login Whitelist** tab.

Constraints

Any of the premium, WTP, or CGS editions must be enabled.

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, click , select a region, and choose **Security > Host Security Service**.

Step 3 Choose **Detection > Whitelists > Login Whitelist** to access the **Whitelists** page, and click **Add**.

Step 4 On the displayed page, enter the server IP address, login IP address, and login username.

Table 7-7 Login security whitelist parameters

Parameter	Description	Example Value
Server IP Address	<ul style="list-style-type: none">IPv4 addresses are supportedSingle IP addresses, IP address segments, and masks are supported. Use commas (,) to separate them.	<ul style="list-style-type: none">192.168.1.1192.168.2.1-192.168.6.1192.168.7.0/24
Login IP Address		
Login Username	Current login username	hss_test

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 its **Operation** column.

 **NOTE**

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

7.2.2 Managing the Alarm Whitelist

You can configure the alarm whitelist to reduce false alarms. Events can be deleted from the whitelist.

Whitelisted events will not trigger alarms.

On the **Alarms** page, you can add falsely reported alarms to the alarm whitelist. After an alarm is added to the whitelist, HSS will not generate alarms or collect statistics on it.

Constraints

Any of the premium, WTP, or CGS editions must be enabled.

Adding Events to the Alarm Whitelist

Table 7-8 Configuring the alarm whitelist

Method	Description
Add to alarm whitelist	<p>Choose to add the alarm to the whitelist when handling it. The following types of events can be added to the alarm whitelist:</p> <ul style="list-style-type: none"> • Reverse shells • Ransomware • Malicious programs • Web shell • Abnormal process behaviors • Process privilege escalations • File privilege escalations • High-risk command executions • Malicious programs • Important file changes • File/Directory changes • Abnormal shells • Suspicious crontab tasks • Invalid accounts • Common vulnerability exploits

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, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane on the left, choose **Detection > Whitelists**.
- Step 4** Click **Alarm Whitelist** to view the added alarm whitelist. For more information, see [Table 7-9](#).

Table 7-9 Parameter description

Parameter Name	Description
Alarm Type	Name of the alarm whitelist type.
SHA256	Hash value of the target file.

----End

Follow-Up Procedure

Removing alarms from the whitelist

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

NOTE


- Exercise caution when performing this operation. Whitelisted alarms cannot be restored after removal, and will be reported once triggered.
- After an alarm is deleted from the whitelist, the handling status of the events associated with the alarm is not updated. To change the status, choose **Detection > Alarms**, click **Handle** in the **Operation** column of an event, and select **Remove from whitelist**.

7.2.3 Configuring the System User Whitelist

HSS generates risky account alarms when non-root users are added to the root user group. You can add the trusted non-root users to the system user whitelist. HSS does not generate risky account alarms for users in the system user whitelist.

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Detection > Whitelists**. The **Whitelists** page is displayed.

Step 4 Click the **System User Whitelist** tab and click **Add**.

Step 5 In the **Add to System User Whitelist** dialog box, enter the server ID, system username, and remarks.

Step 6 Click **OK**.

----End

Related Operations

Modifying a System User Whitelist

Step 1 In the row of the target system user whitelist, click **Modify** in the **Operation** column.

Step 2 In the **Modify System User Whitelist** dialog box, modify the information and click **OK**.

----End

Deleting a System User Whitelist

Step 1 In the row of the target system user whitelist, click **Delete** in the **Operation** column.

You can also select multiple system user whitelists and click **Delete** in the upper left corner of the system user whitelist list.

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

----End

8 Security Operations

8.1 Policy Management

8.1.1 Viewing a Policy Group

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

Constraints

The enterprise, premium, WTP, or container edition is enabled.

Before You Start

- When you enable the enterprise edition, the tenant-side policy group of this edition (including weak password and website shell detection policies) takes effect for all your servers.
- When you enable the premium edition separately, or enabled the premium edition included with the WTP edition, the tenant-side policy group of this edition takes effect.

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

Policy List

Policy Name	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	CGS Edition
Asset Discovery	Scan and display all software in one place, including software name, path, and major applications, helping you identify abnormal assets.	Linux and Windows	×	√	√	√
AV Detection	<p>Check server assets and report, isolate, and kill the detected viruses.</p> <p>The generated alarms are displayed under Detection > Alarms > Server Alarms > Event Types > Malware.</p> <p>After AV detection is enabled, the resource usage is as follows:</p> <p>The CPU usage does not exceed 40% of a single vCPU. The actual CPU usage depends on the server status.</p>	Windows	√	√	√	×
Configuration Check	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS.	Linux and Windows	×	√	√	√
Container Information Collection	Collect information about all containers on a server, including ports and directories, and report alarms for risky information.	Linux	×	×	×	√
Weak Password Detection	Change weak passwords to stronger ones based on HSS scan results and suggestions.	Linux	√	√	√	√

Policy Name	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	CGS Edition
Cluster Intrusion Detection	Detect container high-privilege changes, creation in key information, and virus intrusion.	Linux	×	×	×	√
Container escape	Check for and generate alarms on container escapes.	Linux	×	×	×	√
Web Shell Detection	Scan web directories on servers for web shells.	Linux and Windows	√	√	√	√
Container File Monitoring	Detect file access that violates security policies. Security O&M personnel can check whether hackers are intruding and tampering with sensitive files.	Linux	×	×	×	√
Container Processes Whitelist	Check for process startups that violate security policies.	Linux	×	×	×	√
Suspicious Image Behaviors	Configure the blacklist and whitelist and customize permissions to ignore abnormal behaviors or report alarms.	Linux	×	×	×	√
HIPS Detection	Check registries, files, and processes, and report alarms for operations such as abnormal changes.	Windows	√	√	√	√
File Protection	Check the files in the Linux OS, applications, and other components to detect tampering.	Linux	√	√	√	√


Policy Name	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	CGS Edition
Login Security Check	<p>Detect brute-force attacks on SSH, FTP, and MySQL accounts.</p> <p>If the number of brute-force attacks (consecutive incorrect password attempts) from an IP address reaches 5 within 30 seconds, the IP address will be blocked.</p> <p>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.</p>	Linux and Windows	√	√	√	√
Malicious File Detection	<ul style="list-style-type: none"> Reverse shell: Monitor user process behaviors in real time to detect reverse shells caused by invalid connections. Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. 	Linux	√	√	√	√
Port Scan Detection	Detect scanning or sniffing on specified ports and report alarms.	Linux	×	√	√	√

Policy Name	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	CGS Edition
Abnormal processes behaviors	All the running processes on all your servers are monitored for you. You can create a process whitelist to ignore alarms on trusted processes, and can receive alarms on unauthorized process behavior and intrusions.	Linux	×	√	√	√
Root privilege escalation	Detect the root privilege escalation for files in the current system.	Linux	√	√	√	√
Real-time Processes	Monitor the executed commands in real time and generates alarms if high-risk commands are detected.	Linux and Windows	√	√	√	√
Rootkit Detection	Detect server assets and report alarms for suspicious kernel modules, files, and folders.	Linux	√	√	√	√

Policy Name	Action	Supported OS	Enterprise Edition	Premium Edition	WTP Edition	CGS Edition
Self-protection	<p>Protect HSS files, processes, and software from malicious programs, which may uninstall HSS agents, tamper with HSS files, or stop HSS processes.</p> <ul style="list-style-type: none"> Self-protection depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled. Enabling the self-protection policy has the following impacts: <ul style="list-style-type: none"> The HSS agent cannot be uninstalled on the control panel of a server, but can be uninstalled on the HSS console. HSS process cannot be terminated. In the agent installation path C:\Program Files\HostGuard, you can only access the log and data directories (and the upgrade directory, if your agent has been upgraded). 	Windows	×	√	√	×

Checking the Policy Group List

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Security Operations > Policies** to check the displayed policy groups. For more information, see [Table 8-1](#).

 **NOTE**


- **tenant_linux_container_default_policy_group** is the default Linux policy group of the container edition. This policy group can only be viewed, and cannot be copied or deleted.
 - **tenant_linux_enterprise_default_policy_group** is the default Linux policy group of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted.
 - **tenant_windows_enterprise_default_policy_group** is the default Windows policy group of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted.
 - **tenant_linux_premium_default_policy_group** is the default Linux policy group of the premium edition. You can create a policy group by copying this default group and modify the copy.
 - **tenant_windows_premium_default_policy_group** is the default Windows policy group of the premium edition. You can create a policy group by copying this default group and modify the copy.
 - **wtp_ServerName** is a WTP edition policy group. It is generated by default when WTP is enabled for a server.
- 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.

Table 8-1 Policy group parameters

Parameter	Description
Policy Group	Name of a policy group
ID	Unique ID of a policy group
Description	Description of a policy group
Supported Version	HSS version supported by the policy group.
OS	OS supported by the policy.
Servers	Number of servers associated with the policy

Step 4 Click the name of a policy group to check policy details, including the names, statuses, function categories, OS type of the policies.

 **NOTE**

- All policies in the group **tenant_enterprise_policy_group** are enabled by default.
- You can click **Enable** or **Disable** in the **Operation** column of a policy to control what to check.

Step 5 To view the detailed information about a policy, click the name of the policy.

 NOTE

For details about how to modify a policy, see [Modifying a Policy](#).

----End

8.1.2 Creating a Policy Group

You can create a policy group to perform specific, in-depth scan on certain servers.

Prerequisite

The premium edition has been enabled.


 NOTE

So far, you can create a policy group only in the premium edition. If the premium edition is not enabled for a server, the policy group you create for it will not take effect.

Creating a Policy Group

The following uses a Linux server policy in the premium edition as an example:

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Security Operations > Policies** to check the displayed policy groups. For more information, see [Table 8-2](#).

 NOTE


- **tenant_linux_container_default_policy_group** is the default Linux policy group of the container edition. This policy group can only be viewed, and cannot be copied or deleted.
- **tenant_linux_enterprise_default_policy_group** is the default Linux policy group of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted.
- **tenant_windows_enterprise_default_policy_group** is the default Windows policy group of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted.
- **tenant_linux_premium_default_policy_group** is the default Linux policy group of the premium edition. You can create a policy group by copying this default group and modify the copy.
- **tenant_windows_premium_default_policy_group** is the default Windows policy group of the premium edition. You can create a policy group by copying this default group and modify the copy.
- **wtp_ServerName** is a WTP edition policy group. It is generated by default when WTP is enabled for a server.
- 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.

Table 8-2 Policy group parameters

Parameter	Description
Policy Group	Name of a policy group
ID	Unique ID of a policy group
Description	Description of a policy group
Supported Version	HSS version supported by the policy group.
OS	OS supported by the policy.
Servers	Number of servers associated with the policy

Step 4 Locate the policy group **tenant_linux_premium_default_policy_group** or **tenant_windows_premium_default_policy_group** and click **Copy** in the **Operation** column of the policy group.

The following uses a Linux policy group as an example.

Step 5 In the dialog box displayed, enter a policy group name and description, and click **OK**.

 **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.

Step 6 Click **OK**.

Step 7 Click the name of the policy group you just created. The policies in the group will be displayed.

Step 8 Click a policy name and modify its settings as required. For details, see [Modifying a Policy](#).

Step 9 Enable or disable the policy by clicking the corresponding button in the **Operation** column.

----End

Follow-up Operations

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 Go to the policy list. Delete one or multiple policies.

 **NOTE**

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

You can also select multiple policy groups and click **Delete** above the list to delete them in batches.

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

----End

8.1.3 Modifying a Policy

This section describes how to modify policies in a policy group.

NOTICE


- Modifications on a policy take effect only in the group it belongs to.
- For the default policy groups, you are advised to retain their default configurations.
- Currently, the HIPS policy of Windows servers cannot be modified.

Constraints

The enterprise, premium, WTP, or container edition is enabled.

Accessing the Policies Page

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Security Operations** > **Policies** to check the displayed policy groups. For more information, see [Table 8-3](#).

NOTE


- **tenant_linux_container_default_policy_group** is the default Linux policy group of the container edition. This policy group can only be viewed, and cannot be copied or deleted.
- **tenant_linux_enterprise_default_policy_group** is the default Linux policy group of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted.
- **tenant_windows_enterprise_default_policy_group** is the default Windows policy group of the enterprise edition. This policy group can only be viewed, and cannot be copied or deleted.
- **tenant_linux_premium_default_policy_group** is the default Linux policy group of the premium edition. You can create a policy group by copying this default group and modify the copy.
- **tenant_windows_premium_default_policy_group** is the default Windows policy group of the premium edition. You can create a policy group by copying this default group and modify the copy.
- **wtp_ServerName** is a WTP edition policy group. It is generated by default when WTP is enabled for a server.
- 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.

Table 8-3 Policy group parameters

Parameter	Description
Policy Group	Name of a policy group
ID	Unique ID of a policy group
Description	Description of a policy group
Supported Version	Versions of HSS supported by the policy group
Supported OS	OS supported by the policy.
Servers	Number of servers associated with the policy

Step 4 Click the name of the policy group to access the policy detail list. You can modify the policy by clicking its name.

----End

Asset Discovery

Step 1 Click **Asset Discovery**.

Step 2 On the displayed page, modify the settings as required. For more information, see [Table 8-4](#).

Table 8-4 Parameter description

Parameter	Description
Scan Time	Fixed time for automatic assets scan. <ul style="list-style-type: none">Accounts: Linux accounts are automatically checked every hour, and Windows accounts are checked in real time.Open ports are automatically checked every 30 seconds.Processes are automatically checked every hour.Installed software is automatically checked once a day.Auto-startup items are automatically checked every hour.
Software Scanned	<ul style="list-style-type: none">Software name. A name can contain a maximum of 5,000 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 Scanned	Path for software search. This parameter is not required for Windows servers.

Parameter	Description
Web Directory to Be Scanned	Specifies a web directory to be scanned.
Web Directory Scan Depth	Specifies the level depth for web directory scanning.

Step 3 Confirm the information and click **OK**.

----End

Weak Password Scan

Weak passwords are not attributed to a certain type of vulnerabilities, but they bring no less security risks than any type of vulnerabilities. Data and programs will become insecure if their passwords are cracked.

HSS proactively detects the accounts using weak passwords and generates alarms for the accounts. You can also add a password that may have been leaked to the weak password list to prevent server accounts from using the password.

Step 1 Click **Weak Password Detection**.

Step 2 In the **Policy Settings** area, modify the settings as required. For more information, see [Table 8-5](#).

Table 8-5 Parameter description

Parameter	Description
Scan Time	Time point when detections are performed. It can be accurate to the minute.
Random Deviation Time (s)	Random deviation time of the weak password based on Scan Time . The value range is 0 to 7200s.
Scan Days	Days in a week when weak passwords are scanned. You can select one or more days.
Detection Break Time (ms)	Interval between the checks of two accounts. The value range is 0 to 2,000. For example, if this parameter is set to 50 , the system checks /bin/ls every 50 milliseconds.
User-defined Weak Passwords	You can add a password that may have been leaked to this weak password text box to prevent server accounts from using the password. Enter only one weak password per line. Up to 300 weak passwords can be added.

Step 3 Confirm the information and click **OK**.

----End

Configuration Check

Step 1 Click **Configuration Check**.

Step 2 On the **Configure Check**, modify the policy.

Table 8-6 Parameter description

Parameter	Description
Scan Time	Time point when detections are performed. It can be accurate to the minute.
Random Deviation Time (Seconds)	Random deviation time of the system detection. The value ranges from 0 to 7,200s.
Scan Days	Day in a week when a detection is performed. You can select any days from Monday to Sunday.
System Default Baseline Library	The detection baseline that has been configured in the system. You only need to select the baseline to be scanned.

Step 3 Select the baseline to be detected or customize a baseline.

Step 4 Confirm the information and click **OK**.

----End

Web Shell Detection

If **User-defined Scan Paths** is not specified, the website paths in your assets are scanned by default. If **User-defined Scan Paths** is specified, only the specified paths are scanned.

Step 1 Click **Web Shell Detection**.

Step 2 On the **Web Shell Detection** page, modify the settings as required. For more information, see [Table 8-7](#).

Table 8-7 Parameter description

Parameter	Description
Scan Time	Time point when detections are performed. It can be accurate to the minute.
Random Deviation Time (Seconds)	Random deviation time. The value ranges from 0 to 7,200s.

Parameter	Description
Scan Days	Days in a week when web shells are scanned. You can select one or more days.
User-defined Scan Paths	Web paths to be scanned. A file path must: <ul style="list-style-type: none"> • Start with a slash (/) and end with no slashes (/). • Occupy a separate line and cannot contain spaces.
Monitored Files Types	Extensions of files to be checked. Valid values include jsp, jsp, jspf, php, php5, php4 .

Step 3 Confirm the information and click **OK**.





----End







File Protection

Step 1 Click **File Protection**.

Step 2 On the **File Protection** page, modify the policy. For more information, see [Table 8-8](#).

Table 8-8 Parameter description

Parameter	Description
File Privilege Escalation	<ul style="list-style-type: none"> • Detects privilege escalation. <ul style="list-style-type: none"> -  : enable -  : disable • Ignored File Path: Files to be ignored. Start the path with a slash (/) and do not end it with a slash (/). Each path occupies a line. No spaces are allowed between path names.
File Integrity	<ul style="list-style-type: none"> • Detects the integrity of key files. <ul style="list-style-type: none"> -  : enable -  : disable • File Paths: Configure the file paths.

Parameter	Description
Important File Directory Change	<ul style="list-style-type: none"> • Detects the directory change of key files. <ul style="list-style-type: none"> –  : enable –  : disable • Enable Audit: enables the audit detection function. If the function is enabled and inotify usage exceeds the limit, some file directory changes cannot be detected. <ul style="list-style-type: none"> –  : enable –  : disable • Session IP Whitelist: If the file process belongs to the sessions of the listed IP addresses, no audit applies. • Unmonitored File Types: File types that do not need to be monitored. • Unmonitored File Paths: File paths that do not need to be monitored. • Monitoring Login Keys: enables the function of monitoring login keys. <ul style="list-style-type: none"> –  : enable –  : disable
Directory Monitoring Mode	<ul style="list-style-type: none"> • Directory monitoring mode. • File or Directory Path: Some file or directory monitoring paths are preset in the system. You can modify the file change type to be detected and add the file or directory paths to be monitored.

Step 3 Confirm the information and click **OK**.





----End

Login Security Check

Step 1 Click **Login Security Check**.

Step 2 In the displayed **Login Security Check** page, modify the policy content. [Table 8-9](#) describes the parameters.

Table 8-9 Parameter description

Parameter	Description
Lock Time (min)	This parameter is used to determine how many minutes the IP addresses that send attacks are locked. The value range is 1 to 43200. Login is not allowed in the lockout duration.
Cracking Behavior Determination Threshold (s)	This parameter is used together with Cracking Behavior Determination Threshold (Login Attempts) . The value range is 5 to 3,600. For example, if this parameter is set to 30 and Cracking Behavior Determination Threshold (Login Attempts) is set to 5 , the system determines that an account is cracked when the same IP address fails to log in to the system for five times within 30 seconds.
Cracking Behavior Determination Threshold (Login Attempts)	This parameter is used together with Cracking Behavior Determination Threshold . The value range is 1 to 36,000.
Threshold for slow brute force attack (second)	This parameter is used together with Threshold for slow brute force attack (failed login attempt) . The value range is 600 to 86,400s. For example, if this parameter is set to 3600 and Threshold for slow brute force attack (failed login attempt) is set to 15 , the system determines that an account is cracked when the same IP address fails to log in to the system for fifteen times within 3,600 seconds.
Threshold for slow brute-force attack (failed login attempt)	This parameter is used together with Threshold for slow brute force attack (second) . The value range is 6 to 100.
Check Whether the Audit Login Is Successful	<ul style="list-style-type: none">After this function is enabled, HSS reports login success logs. <p>-  : enable</p> <p>-  : disable</p>
Block Non-whitelisted Attack IP Address	After this function is enabled, HSS blocks the login of brute force IP addresses (non-whitelisted IP addresses).
Report Alarm on Brute-force Attack from Whitelisted IP Address	<ul style="list-style-type: none">After this function is enabled, HSS generates alarms for brute force attacks from whitelisted IP addresses. <p>-  : enable</p> <p>-  : disable</p>

Parameter	Description
Whitelist	After an IP address is added to the whitelist, HSS does not block brute force attacks from the IP address in the whitelist. A maximum of 50 IP addresses or network segments can be added to the whitelist. Both IPv4 and IPv6 addresses are supported.

Step 3 Confirm the information and click **OK**.





----End





Malicious File Detection

Step 1 Click **Malicious File Detection**.

Step 2 On the displayed page, modify the policy. For more information, see [Table 8-10](#).

Table 8-10 Parameter description

Parameter	Description
Whitelist Paths in Reverse Shell Check	Process file path to be ignored in reverse shell detection Start with a slash (/) and end with no slashes (/). Occupy a separate line and cannot contain spaces.
Reverse Shell Scanning Interval (s):	Reverse shell scanning period. The value range is 30 to 86,400.
Audit detection enhancement	<ul style="list-style-type: none"> Whether to enhance audit detection. You are advised to enable this function. -  : 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.
Detect Reverse Shells	<ul style="list-style-type: none"> Detects reverse shells. You are advised to enable it. -  : enable -  : disable

Parameter	Description
Auto-block Reverse Shells	<p>Specifies whether to enable automatic blocking of reverse shells. You are advised to enable this function.</p> <ul style="list-style-type: none">  : enable  : disable <p>NOTE This parameter takes effect after the function of Isolating and Killing Malicious Programs is enabled.</p>
Abnormal Shell Detection	<ul style="list-style-type: none"> • Detects abnormal shells. You are advised to enable it. <ul style="list-style-type: none"> -  : enable -  : disable

Step 3 Confirm the information and click **OK**.

----End

Abnormal Process Behavior

Step 1 Click **Abnormal process behaviors**.

Step 2 In the displayed area, modify the settings as required. For more information, see [Table 8-11](#).

Table 8-11 Parameter description

Parameter	Description	Example Value
Detection and Scanning Cycle (Seconds)	Interval for checking the running programs on the host. The value range is 30 to 1,800.	1800

Parameter	Description	Example Value
Detection Mode	Select the method for abnormal process behavior detection. <ul style="list-style-type: none">• Sensitive: In-depth and full detection and scanning are performed on all processes, which may cause false positives. Suitable for cyber protection drills and key event assurance drills.• Balanced: All processes are detected and scanned. The detection result accuracy and the abnormal process detection rate are balanced. Suitable for routine protection.• Conservative: All processes are detected and scanned. This mode provides high detection result accuracy and low false positives. Suitable for scenarios with a large number of false positives.	Balanced

Step 3 Confirm the information and click **OK**.

----End

Root Privilege Escalation Detection

Step 1 Click **Root privilege escalation**.

Step 2 In the displayed area, modify the settings as required. For more information, see [Table 8-12](#).

Table 8-12 Parameter description

Parameter	Description
Ignored Process File Path	Ignored process file path Start with a slash (/) and end with no slashes (/). Occupy a separate line and cannot contain spaces.
Scanning Interval (s)	Interval for checking process files. The value range is 5 to 3,600.

Step 3 Confirm the information and click **OK**.

----End

Real-time Process

Step 1 Click **Real-time Process**.

Step 2 On the displayed page, modify the settings as required. For more information, see [Table 8-13](#).

Table 8-13 Parameters for real-time process policy settings

Parameter	Description
Full Process Report Interval (s)	Interval for reporting the full process. The value range is 3,600 to 86,400.
High-Risk Commands	High-risk commands that contain keywords during detection.
Whitelist (Do Not Record Logs)	Add paths or program names that are allowed or ignored during detection.

Step 3 Confirm the information and click **OK**.







----End

Rootkit Detection

Step 1 Click **Rootkit Detection**.

Step 2 On the rootkit detection page, modify the policy content.

Table 8-14 Parameter description

Parameter	Description	Example Value
Scanning Interval (s)	Interval for executing the check policy. The value ranges from 60 to 86,400.	86400
Check Library	Check files and folders in the existing libraries. You are advised to enable this function. <ul style="list-style-type: none">  : enable  : disable 	 : enable
Check Kernel Space	Perform the check by kernel modules. All kernel modules will be checked. You are advised to enable this function. <ul style="list-style-type: none">  : enable  : disable 	 : enable
Kernel Module Whitelist	Add the kernel modules that can be ignored during the detection. Up to 10 kernel modules can be added. Each module occupies a line.	xt_contrack virtio_scsi tun

Step 3 Confirm the information and click **OK**.




----End

AV Detection

Step 1 Click **AV Detection**.

Step 2 On the **AV Detection** slide pane that is displayed, modify the settings as required. For details, see [Table 8-15](#).

Table 8-15 AV detection policy parameters

Parameter	Description	Example Value
Real-Time Protection	<p>After this function is enabled, AV detection is performed in real time when the current policy is executed. You are advised to enable this function.</p> <ul style="list-style-type: none">  : enable  : disable 	
Protected File Type	<p>Type of the files to be checked in real time.</p> <ul style="list-style-type: none"> All: Select all file types. Executable: Executable file types such as EXE, DLL, and SYS. Compressed: Compressed file types such as ZIP, RAR, and JAR. Text: Text file types such as PHP, JSP, HTML, and Bash. OLE: Composite file types such as Microsoft Office files (PPT and DOC) and saved email files (MSG). Other: File types except the preceding types. 	All
Action	<p>Handling method for the object detection alarms.</p> <ul style="list-style-type: none"> Automated handling: Isolate high-risk virus files by default. Report other virus files but do not isolate them. Manual handling: Report all the detected virus files but do not isolate them. You need to handle them manually. 	Automated handling

Step 3 Confirm the information and click **OK**.

----End

Container Information Collection

Step 1 Click **Container Information Collection**.

Step 2 On the **Container Information Collection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see [Table 8-16](#).

 **NOTE**

The whitelist has a higher priority than blacklist. If a directory is specified in both the whitelist and blacklist, it is regarded as a whitelisted item.

Table 8-16 Container information collection policy parameters

Parameter	Description	Example Value
Mount Path Whitelist	Enter the directory that can be mounted.	/test/docker or /root/* Note: If a directory ends with an asterisk (*), it indicates all the sub-directories under the directory (excluding the main directory).
Mount Path Blacklist	Enter the directories that cannot be mounted. For example, user and bin , the directories of key host information files, are not advised being mounted. Otherwise, important information may be exposed.	For example, if /var/test/* is specified in the whitelist, all sub-directories in /var/test/ are whitelisted, excluding the test directory.

Step 3 Confirm the information and click **OK**.

----End

Cluster Intrusion Detection

Step 1 Click **Cluster Intrusion Detection**.

Step 2 On the **Cluster Intrusion Detection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see [Table 8-17](#).

Table 8-17 Cluster intrusion detection policy parameters

Parameter	Description	Example Value
Basic Detection Cases	Select basic check items as required.	Select all

Parameter	Description	Example Value
Whitelist	<p>You can customize the types and values that need to be ignored during the detection. You can add and delete types and values as required.</p> <p>The following types are supported:</p> <ul style="list-style-type: none">• IP address filter• Pod name filter• Image name filter• User filter• Pod tag filter• Namespace filter <p>NOTE Each type can be used only once.</p>	<p>Type: IP address filtering Value: 192.168.x.x</p>

 **NOTE**

After this policy is configured, you need to enable the log audit function and deploy the HSS agent on the management node (node where the APIServer is located) of the cluster to make the policy take effect.

Step 3 Confirm the information and click **OK**.

----End

Container File Monitoring

NOTICE

If a monitored file path is under the mount path rather than the writable layer of the container on the server, changes on the file cannot trigger container file modification alarms. To protect such files, configure a [file protection policy](#).

Step 1 Click **Container File Monitoring**.

Step 2 On the **Container File Monitoring** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see [Table 8-18](#).

Table 8-18 Container file monitoring policy parameters

Parameter	Description	Example Value
Fuzzy match	Indicates whether to enable fuzzy match for the target file. You are advised to select this option.	Selected
Block New Executable	Monitor the behavior of the adding executable files. If this option is selected, adding executable files is prohibited. You are advised to select this option.	Selected
Image Name	Name of the target image to be checked	test_bj4
Image ID	ID of the target image to be checked	-
File	Name of the file in the target image to be checked	/tmp/testw.txt

Step 3 Confirm the information and click **OK**.

----End

Container Process Whitelist

Step 1 Click **Container Process Whitelist**.

Step 2 On the **Container Process Whitelist** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see [Table 8-19](#).

Table 8-19 Container process whitelist policy parameters

Parameter	Description	Example Value
Fuzzy Match	Indicates whether to enable fuzzy match for the target file. You are advised to select this option.	Selected
Image Name	Name of the target image to be detected	test_bj4
Image ID	ID of the target image to be checked	-
Process	Path of the file in the target image to be checked	/tmp/testw

Step 3 Confirm the information and click **OK**.

----End

Suspicious Image Behaviors

Step 1 Click **Suspicious Image Behaviors**.

Step 2 On the **Suspicious Image Behaviors** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see [Table 8-20](#).

Table 8-20 Suspicious image behaviors policy parameters

Parameter	Description	Example Value
Rule Name	Name of a rule	-
Description	Brief description of a rule	-
Template	<ul style="list-style-type: none">• Configure templates based on different rules. The supported rules are as follows:<ul style="list-style-type: none">- Image whitelist- Image blacklist- Image tag whitelist- Image tag blacklist- Create container whitelist- Create container blacklist- Container mount proc whitelist- Container seccomp unconfined- Container privilege whitelist- Container capability whitelist• The parameters are described as follows:<ul style="list-style-type: none">- Exact match: Enter the names of the images you want to check. Use semicolons (;) to separate multiple names. A maximum of 20 names can be entered.- RegEx match: Use regular expressions to match images. Use semicolons (;) to separate multiple expressions. A maximum of 20 expressions can be entered.- Prefix match: Enter the prefixes of the images you want to check. Multiple prefixes are separated by semicolons (;). A maximum of 20 prefixes can be entered.- Tag Name: Enter the tag and value of the images you want to check. A maximum of 20 tags can be added.- Permission Type: Specify permissions to be checked or ignored. For details about permissions, see Table 8-21.	-

Table 8-21 Abnormal image permissions

Permissions Name	Description
AUDIT_WRITE	Write records to kernel auditing log.
CHOWN	Make arbitrary changes to file UIDs and GIDs.
DAC_OVERRIDE	Bypass file read, write, and execute permission checks.
FOWNER	Bypass permission checks on operations that normally require the file system UID of the process to match the UID of the file.
FSETID	Do not clear set-user-ID and set-group-ID permission bits when a file is modified.
KILL	Bypass permission checks for sending signals
MKNOD	Create special files using mknod.
NET_BIND_SERVICE	Bind a socket to internet domain privileged ports (port numbers less than 1024).
NET_RAW	Use RAW and PACKET sockets.
SETFCAP	Set file capabilities.
SETGID	Make arbitrary manipulations of process GIDs and supplementary GID list.
SETPCAP	Modify process capabilities.
SETUID	Make arbitrary manipulations of process UIDs.
SYS_CHROOT	Use chroot to change the root directory.
AUDIT_CONTROL	Enable and disable kernel auditing; change auditing filter rules; retrieve auditing status and filtering rules.
AUDIT_READ	Allow reading audit logs via multicast netlink socket.
BLOCK_SUSPEND	Allow suspension prevention.
BPF	Allow creating BPF maps, loading BPF Type Format (BTF) data, retrieve JITed code of BPF programs, and more.
CHECKPOINT_RESTORE	Allow operations related to checkpoints and restoration.
DAC_READ_SEARCH	Bypass file read permission checks and directory read and execute permission checks.
IPC_LOCK	Lock memory (such as mlock, mlockall, mmap, and shmctl).

Permissions Name	Description
IPC_OWNER	Bypass permission checks for operations on System V IPC objects.
LEASE	Establish leases on arbitrary files
LINUX_IMMUTABLE	Set the FS_APPEND_FL and FS_IMMUTABLE_FL i-node flags.
MAC_ADMIN	Allow MAC configuration or state changes.
MAC_OVERRIDE	Override Mandatory Access Control (MAC).
NET_ADMIN	Perform various network-related operations.
NET_BROADCAST	Make socket broadcasts, and listen to multicasts.
PERFMON	Allow privileged system performance and observability operations using perf_events, i915_perf and other kernel subsystems.
SYS_ADMIN	Perform a range of system administration operations.
SYS_BOOT	Use reboot and kexec_load. Reboot and load a new kernel for later execution.
SYS_MODULE	Load and unload kernel modules.
SYS_NICE	Raise process nice value (nice, set priority) and change the nice value for arbitrary processes.
SYS_PACCT	Enable or disable process accounting.
SYS_PTRACE	Trace arbitrary processes using ptrace.
SYS_RAWIO	Perform I/O port operations (iopl and ioperm).
SYS_RESOURCE	Override resource limits.
SYS_TIME	Set the system clock (settimeofday, stime, and adjtimex) and real-time (hardware) clock.
SYS_TTY_CONFIG	Use vhangup. Employ various privileged ioctl operations on virtual terminals.
SYSLOG	Perform privileged syslog operations.
WAKE_ALARM	Trigger something that will wake up the system.

Step 3 Confirm the information and click **OK**.

----**End**

Port Scan Detection

- Step 1** Click **Port Scan Detection**.
- Step 2** On the **Port Scan Detection** slide pane that is displayed, modify the **Policy Settings**. For details about the parameters, see [Table 8-22](#).

Table 8-22 Port scan detection policy parameters

Parameter	Description	Example Value
Process Information Collection Interval (s):	Interval for obtaining processes	Selected
Source IP Address Whitelist	Enter the IP address whitelist. Separate multiple IP addresses with semicolons (;).	test_bj4
Packet Quantity Threshold	-	-
Ports to Scan	Details about the port number and protocol type to be detected	-

- Step 3** Confirm the information and click **OK**.

----End


Self-protection


The self-protection policy protects HSS software, processes, and files from being damaged by malicious programs. You cannot customize the policy content.

8.2 Viewing the Handling History

You can check the handling history of vulnerabilities, including their handlers and handling time.

Viewing the Handling History of all Vulnerabilities

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page, select a region, and choose **Security** > Host Security Service.
- Step 3** In the navigation pane on the left, choose **Security Operations** > **Handling History**.
- Step 4** On the **Vulnerabilities** tab page displayed, view the handling history of all vulnerabilities.

- Viewing the vulnerability handling history of a specified property
In the search box above the vulnerability handling history list, enter a vulnerability type, vulnerability name, or server IP address, and click  to view the vulnerability handling history of a specified property.

----End

9 Security Report

9.1 Checking a Security Report

You can subscribe to **daily**, weekly, monthly, and **custom** reports. The reports show your server security trends and key security events and risks.

 **NOTE**


After you subscribe to a report, it will be available for review and download the next day.

Constraints

The enterprise, premium, WTP, or container edition is enabled.

Security Report Overview

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 4 Click **Download** to go to the preview page. You can check the information of the target report and download or send it.

----End

Checking Report History

The report history stores the report sending details.

Step 1 In the upper right corner of the security report overview page, click **Report History** to check the report sending records.

- Step 2** Check the report history on the displayed page, as shown in the following picture. For more information, see [Table 9-1](#).

Table 9-1 Parameter description

Parameter	Description
Report Name	Name of a sent report.
Statistical Period	Statistical period of a sent report.
Report Type	Statistical period type of a sent report. <ul style="list-style-type: none">• Weekly Reports• Monthly Reports• Daily Reports• Custom Reports
Sent	Time when the report is sent.

- Step 3** Click **Download** in the **Operation** column to check historical reports. You can also preview and download the reports.

----End

9.2 Subscribing to a Security Report

This section provides guidance for you to quickly subscribe to weekly or monthly security reports using preset templates on the console. For details about how to customize a security report, see [Creating a Security Report](#).


Constraints

The enterprise edition and higher editions support operations related to security reports.

Precaution

- A security report is generated for all protected servers. You cannot specify a server and generate a security report for it.
- Subscription to security reports is free of charge, but the report content varies depending on the quota edition you use.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.

Step 3 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 4 You can subscribe to monthly or weekly security reports. For details about how to edit a report, see [Editing a Report](#).

----End

9.3 Creating a Security Report


If the type and content of the existing report template cannot meet your requirements, you can customize a report.

Constraints

The enterprise edition and higher editions support operations related to security reports.

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 4 Create a report.

- Create a monthly or weekly security report based on templates.
 - Click **Copy** in the weekly or monthly report card to access the basic information configuration page.
- You can also customize the report period.
 - Click **Create Report** to access the basic information configuration page.

Step 5 Edit basic information of a report. For more information, see [Table 9-2](#).

Table 9-2 Parameter description

Parameter	Description	Example Value
Report Name	Default report name	ecs security report

Parameter	Description	Example Value
Report Type	Statistical period type of a report: <ul style="list-style-type: none">• Daily: 00:00 to 24:00 every day• Weekly Reports: 00:00 on Monday to 24:00 on Sunday• Monthly Reports: 00:00 on the first day to 24:00 on the last day of each month• Custom: custom statistical period, which ranges from one day to three months• All types of reports will be sent to the recipients the day after it is generated.	Monthly Reports
Schedule Delivery	Time when a report is automatically sent	-
Send Report To	Security report recipients. <ul style="list-style-type: none">• Recipients specified in SMN topic: If you use SMN topic settings, you can create a topic and specify recipients for HSS.• No need to send to email: The report is not sent to the specified email address.	Recipients specified in SMN topic

Step 6 After confirming that the information is correct, click **Next** in the lower right corner of the page to configure the report.

Step 7 Select the report items to be generated in the left pane. You can preview the report items in the right pane. After confirming the report items, click **Save**, and enable security report subscription.

----End

9.4 Managing a Security Report


This section describes how to modify, cancel, or disable a subscribed report.

Constraints

The enterprise edition and higher editions support operations related to security reports.

Editing a Report

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 4 Click **Edit** in the lower right corner of the target report.

Step 5 Edit basic information of a report. For more information, see [Table 9-3](#).

Table 9-3 Parameter description

Parameter	Description	Example Value
Report Name	Default report name.	default monthly security report
Report Type	Name of the statistical period type of a report, which cannot be edited.	Monthly Reports
Schedule Delivery	Time when a report is automatically sent.	-
Send Report To	Mode to send the generated security reports: <ul style="list-style-type: none"> Recipients specified in SMN topic: If you use SMN topic settings, you can create a topic and specify recipients for HSS. No need to send to email: The report is not sent to the specified email address. 	Recipients specified in SMN topic

Step 6 Confirm the information and click **Next** in the lower right corner of the page to configure the report.

Step 7 Select or deselect the report items in the pane on the left. You can preview the report items on the right. After confirming the report items, click **Save**. The report is changed successfully.


----End

Unsubscribing from a Report

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 3 Toggle off the target report ().

----End

Deleting a Report

NOTE

Default security report templates **default monthly security report** and **default weekly security report** cannot be deleted.

Step 1 Log in to the management console and go to the HSS page.

Step 2 In the navigation pane on the left, choose **Reports**. The security report overview page is displayed.

You can use default security report templates directly, which are **default monthly security report** and **default weekly security report**.

Step 3 Click **Delete** in the lower right corner of the target report.

----End


10 Installation & Configuration

10.1 Agent Management

10.1.1 Viewing Agent Management

You can sort servers, check whether the agent is installed on them, and can install or uninstall the agent. On the console, you can find the agent installation instructions and the link to the agent package.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.
- Step 4** Click **Offline** to check the servers where the agent is not installed or is offline. Click **Online** to check the servers where the agent is online.
- Step 5** Click **Installation Guide** to check the guide for installing the agent.
- Step 6** Click **Agent Version Information** to view the latest version, earlier versions, and changes of the agent.

----End

10.1.2 Installing an Agent

Install the agent on a server. Only then can the server be protected by HSS.

Installation Precautions

- For details about the OSs supported by the agent, see [Supported OSs](#).
- Ensure the outbound rule of your security group allows access to the port 10190 on the 100.125.0.0/16 network segment. (This is the default setting.)

- If any third-party security software has been installed on your server, the HSS agent may fail to be installed. In this case, disable or uninstall the software before installing the agent.
- The available capacity of the disk where the agent is installed must be greater than 300 MB. Otherwise, the agent installation may fail.
- After the installation, it takes 5 to 10 minutes to update the agent status. You can check it on the "Servers" tab of the "Asset Management > Servers & Quota" page.

Installing an Agent on a Server


- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.
- Step 4** Click **Offline** to check the servers where the agent is not installed or is offline. [Table 10-1](#) describes the parameters.

Table 10-1 Offline agent parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	EIP or private IP address of a server
OS	Server OS. Its value can be: <ul style="list-style-type: none">• Linux• Windows
Agent Status	Agent status of a server. Its value can be: <ul style="list-style-type: none">• Offline• Not installed• Installation failed

- Step 5** Click **View Cause** in the **Operation** column of a server to check why an agent is offline.
- Step 6** Click **Install Agent** in the **Operation** column. Download the agent package suitable for your server architecture and OS. For details about how to install the agent on a Linux server, see [Installing an Agent on Linux](#). For details about how to install the agent on a Windows server, see [Installing an Agent on Windows](#).

----End

10.1.3 Uninstalling an Agent

If you no longer need to use HSS, uninstall the agent by following the instructions provided in this section. If the agent is uninstalled, HSS will stop protecting your servers and detecting risks.

Uninstallation Methods

The agent can be uninstalled in one click on the console or manually uninstalled.

- Agent uninstallation on the console: If the agent is online, you can uninstall it in one click on the console.
 - [Uninstalling the Agent from a Single Server in One Click](#)
 - [Uninstalling the Agent from Multiple Servers in One Click](#)
- Manual agent uninstallation: If the agent is offline, you can manually uninstall it.
 - [Manually Uninstalling the Agent from a Linux Server](#)
 - [Manually Uninstalling the Agent from a Windows Server](#)

Uninstalling the Agent from a Single Server in One Click


- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.
- Step 4** Click **Offline** to check the servers where the agent is online. [Table 10-2](#) describes the parameters.

Table 10-2 Online agent parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	EIP or private IP address of a server
OS	Server OS. Its value can be: <ul style="list-style-type: none">• Linux• Windows
Agent Status	Agent status of a server. Its value can be: <ul style="list-style-type: none">• Online
Agent Version	Version of the agent installed on the target server.


Parameter	Description
Agent Upgrade Status	The agent upgrade status.

Step 5 Click **Uninstall Agent** in the **Operation** column of a server. In the dialog box that is displayed, confirm the uninstallation information and click **OK**.

----End

Uninstalling the Agent from Multiple Servers in One Click

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.

Step 4 Click **Offline** to check the servers where the agent is online. [Table 10-3](#) describes the parameters.

Table 10-3 Online agent parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	EIP or private IP address of a server
OS	Server OS. Its value can be: <ul style="list-style-type: none"> • Linux • Windows
Agent Status	Agent status of a server. Its value can be: <ul style="list-style-type: none"> • Online
Agent Version	Version of the agent installed on the target server.
Agent Upgrade Status	The agent upgrade status.

Step 5 Select the target servers whose agent you want to uninstall.

 **NOTE**

If you check the box before **Server Name/ID**, all servers on the page will be selected.

Step 6 Click **Uninstall Agent** above the server list. In the dialog box displayed, confirm the servers from which you want to uninstall the agent and click **OK**.

----End

Manually Uninstalling the Agent from a Linux Server

Step 1 Remotely log in to the Linux server where the agent is to be uninstalled.

- 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, WinSCP, PuTTY, or Xshell, to log in to the server and install the agent on the server as user **root**.

Step 2 If the agent has been installed, run the following command to uninstall it:

 **NOTE**

Do not run the uninstallation command in the `/usr/local/hostguard/` directory. You can run the uninstallation command in any other directory.

- For EulerOS, CentOS, and Red Hat, or other OSs that support RPM installation, run the `rpm -e hostguard;` command.
- For Ubuntu, Debian, and other OSs that support DEB installation, run the `dpkg -P hostguard;` command.

Step 3 Verify the uninstallation. If the `/usr/local/hostguard/` directory is not found on the Linux server, the agent has been uninstalled.

----End

Manually Uninstalling the Agent from a Windows Server

Step 1 Remotely log in to the Windows server where the agent is to be uninstalled.

- 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 mstsc or RDP, to log in to the server and install the agent on the server as an administrator.

Step 2 Go to `C:\Program File\HostGuard` on the Windows server.

Step 3 Double-click the `unins000.exe` file to uninstall the agent.

Step 4 In the **HostGuard Uninstall** dialog box, click **Yes** to delete HostGuard and all its components.

Step 5 (Optional) Restart the server.

- If you have enabled WTP, you need to restart the server after uninstalling the agent. In the **HostGuard Uninstall** dialog box, click **Yes** to restart the server.
- If you have not enabled WTP, you do not need to restart the server. In the **HostGuard Uninstall** dialog box, click **No** to skip server restart.

Step 6 If the **C:\Program Files\HostGuard** directory does not exist on the Windows server, the agent has been uninstalled.


----End

10.1.4 Upgrading the Agent

HSS keeps improving its service capabilities, including but not limited to new features and defect fixes. Please upgrade your agent to the latest version in a timely manner to enjoy better service.

Upgrading the Agent on a Server

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.

Step 4 Click **Offline** to check the servers where the agent is online. [Table 10-4](#) describes the parameters.

Table 10-4 Online agent parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	EIP or private IP address of a server
OS	Server OS. Its value can be: <ul style="list-style-type: none">• Linux• Windows
Agent Status	Agent status of a server. Its value can be: <ul style="list-style-type: none">• Online
Agent Version	Version of the agent installed on the target server.
Agent Upgrade Status	The agent upgrade status.


Step 5 Click **Upgrade** in the **Operation** column of the target server. In the dialog box displayed, confirm the upgrade details and click **OK**.

Step 6 After the upgrade completes, check the agent version. If the latest version agent is used, the upgrade is successful.

----End

Upgrading the Agent on Multiple Servers

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Installation & Configuration**. Click the **Agents** tab.

Step 4 Click **Offline** to check the servers where the agent is online. [Table 10-5](#) describes the parameters.

Table 10-5 Online agent parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	EIP or private IP address of a server
OS	Server OS. Its value can be: <ul style="list-style-type: none">• Linux• Windows
Agent Status	Agent status of a server. Its value can be: <ul style="list-style-type: none">• Online
Agent Version	Version of the agent installed on the target server.
Agent Upgrade Status	The agent upgrade status.

Step 5 Select the target servers whose agent you want to upgrade.

 **NOTE**

- If you check the box before **Server Name/ID**, all servers on the page will be selected.
- If you check the box before **Select all**, all servers you have will be selected.

Step 6 Click **Upgrade Agent** above the server list. In the dialog box displayed, confirm server information and click **OK**.

Step 7 After the upgrade completes, check the agent version. If the latest version agent is used, the upgrade is successful.

----End

10.2 Security Configurations

You can add common login locations, common IP addresses, and whitelist IP addresses, and enable malicious program isolation and killing to enhance server security.

For details, see [Installation and Configuration](#).

10.3 Plug-in Management

10.3.1 Plug-Ins Overview

You can install and manage plug-ins.

Plug-in Type

Currently, only Docker plug-ins can be managed.

Docker Plug-in Application Scenarios

If container protection is enabled and you want to use the image blocking function, you need to [install the Docker plug-in](#).

The Docker plug-in provides the image blocking capability. It can prevent the startup of container images that have high-risk vulnerabilities or do not comply with security standards in the Docker environment.

You can configure image blocking in the following scenarios:


- To enhance the security of container images and prevent the risks caused by the use of untrusted or outdated images, you can configure an [image blocking policy](#) to specify the level of vulnerabilities to be blocked or the whitelist.
- If you need to comply with the security requirements of certain industries or regulations, such as PCI DSS and CIS, you can [configure an image blocking policy](#) to specify the security baseline or compliance check items to be blocked.
- If you need to implement the best practices of container DevSecOps and embed security check and defense into each phase of the container lifecycle, you can [configure an image blocking policy](#) to enhance security from source to devices.

10.3.2 Viewing Plug-in Details

You can view the details about the plug-ins used by servers.

You can install, upgrade, and uninstall plug-ins as required.

Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane on the left, choose **Installation & Configuration** and click the **Plug-in Settings** tab to view details about all plug-ins. For more information, see [Table 10-6](#).

By default, all servers are displayed in the plug-in list. If a plug-in is installed on a server, the plug-in details are displayed. If no plug-ins are installed on a server, the plug-in information is empty.

Table 10-6 Docker plug-in list parameters

Parameter	Description
Server Name/ID	Server name and ID
IP Address	Server IP address
OS	Type of the OS running on the server
Plug-in Name	Name of the plug-in installed on the server.
Plug-in Version	Name of the plug-in installed on the server.
Plug-in Status	Current status of the plug-in. <ul style="list-style-type: none">● Created: The plug-in has been created but has not been started.● Running: The plug-in is running properly.● Paused: The plug-in is paused.● Restarting: The plug-in is being restarted.● Removing: The plug-in is being deleted.● Exited: The plug-in has been stopped.● Dead: The plug-in cannot be started or has been deleted.
Plug-in Upgrade Status	Plug-in upgrade status. <ul style="list-style-type: none">● Not upgraded: The plug-in has not been upgraded to the latest version.● Upgrading: The plug-in is being upgraded.● Upgraded: The plug-in has been upgraded.● Upgrade failed: The plug-in failed to be upgraded.

----End

10.3.3 Installing a Plug-in


If container protection is enabled and you want to use the image blocking function, install the Docker plug-in by following the instructions provided in this section.

Constraints

- Only Docker containers are supported. Containerd containers are not supported.
- The Docker engine version is 18.06.0 or later.
- The Docker API version is 1.38 or later.
- Only Linux servers are supported.
- Only the x86 and Arm hardware architectures are supported.
- The HSS container edition has been enabled.

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Installation & Configuration** and click the **Plug-in Settings > Docker plug-in** tab. Click **Plug-in installation guide**, obtain the installation commands from the slide-out panel, and click **Copy**.

Step 4 Remotely log in to the server where the plug-in is to be installed as the **root** user.

- 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 PuTTY or Xshell, to log in to the server and install the plug-in on the server as user **root**.

Step 5 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 6 Create **linux-host-list.txt**, which will contain the server private IP addresses where the agent is to be installed:

Command syntax:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt  
Or  
echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

To specify multiple IP addresses, write multiple commands, each in a separate line.

Example:

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt  
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt  
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

Step 7 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 8 Copy the batch installation commands to the command terminal and press **Enter**.

Step 9 If **remote_install finished. [OK]** is displayed, the installation is successful. Wait for 3 to 5 minutes and choose **Installation & Configuration** and click the **Plug-in Settings** tab to check the Docker plug-in status of the panel server.

```
remote_install finished. [OK]
```

----End

10.3.4 Upgrading a Plug-in


You can upgrade plug-ins of a target server.

Constraints

- Only Docker containers are supported. Containerd containers are not supported.
- The Docker engine version is 18.06.0 or later.
- The Docker API version is 1.38 or later.
- Only Linux servers are supported.
- Only the x86 and Arm hardware architectures are supported.
- The HSS container edition has been enabled.

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Installation & Configuration** and click the **Plug-in Settings > Docker plug-in** tab. Click **Plug-in upgrade guide**, obtain the upgrade commands from the slide-out panel, and click **Copy**.

Step 4 Remotely log in to the server where the plug-in is to be upgraded as the **root** user.

- 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 PuTTY or Xshell, to log in to the server and upgrade the plug-in on the server as user **root**.

Step 5 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 6 Create **linux-host-list.txt**, which will contain the server private IP addresses where the plug-in is to be upgraded:

Command syntax:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt  
Or echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

To specify multiple IP addresses, write multiple commands, each in a separate line.

Example:

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

Step 7 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 8 Copy the batch upgrade commands to the command box and press **Enter**. The upgrade starts automatically.

Step 9 If **remote_upgrade finished. [OK]** is displayed, the upgrade is successful. Wait for 3 to 5 minutes and choose **Installation & Configuration** and click the **Plug-in Settings** tab to check the Docker plug-in status of the panel server.

```
remote_upgrade finished. [OK]
```

----End


10.3.5 Uninstalling a Plug-in

Constraints

- Only Docker containers are supported. Containerd containers are not supported.
- The Docker engine version is 18.06.0 or later.
- The Docker API version is 1.38 or later.
- Only Linux servers are supported.
- Only the x86 and Arm hardware architectures are supported.
- The HSS container edition has been enabled.

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Installation & Configuration** and click the **Plug-in Settings > Docker plug-in** tab. Click **Plug-in uninstallation guide**, obtain the uninstallation commands from the slide-out panel, and click **Copy**.

Step 4 Remotely log in to the server where the plug-in is to be uninstalled as the **root** user.

- 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 PuTTY or Xshell, to log in to the server and uninstall the plug-in on the server as user **root**.

Step 5 Run the following command to access the **/tmp** directory:

```
cd /tmp/
```

Step 6 Create **linux-host-list.txt**, which will contain the server private IP addresses where the plug-in is to be uninstalled:

Command syntax:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt  
Or echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

To specify multiple IP addresses, write multiple commands, each in a separate line.

Example:

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt  
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt  
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

Step 7 Press **Enter** to save the IP address. Run the **cat linux-host-list.txt** command to verify the IP addresses have been added.

Step 8 Copy the batch uninstallation commands to the command box and press **Enter**. The uninstallation starts automatically.

Step 9 If **remote_uninstall finished. [OK]** is displayed, the uninstallation is successful. Wait for 3 to 5 minutes and choose **Installation & Configuration** and click the **Plug-in Settings** tab to check the Docker plug-in status of the panel server.

```
remote_uninstall finished. [OK]
```

----End

11 Permissions Management

11.1 Creating a User and Granting Permissions

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

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

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

This section describes the procedure for granting permissions (see [Figure 11-1](#)).

Prerequisite

Before authorizing permissions to a user group, you need to know which HSS permissions can be added to the user group. [Table 11-1](#) describes the policy details.

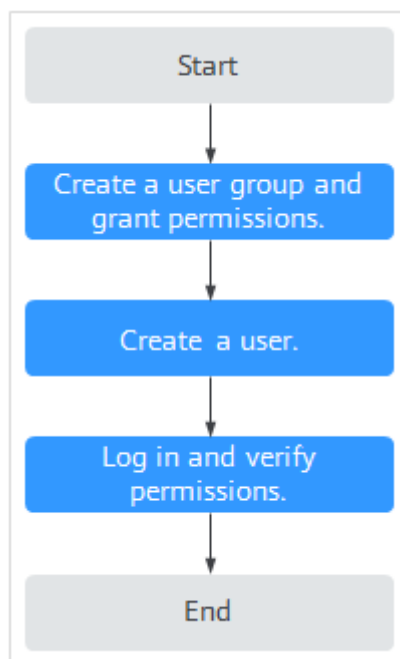
Table 11-1 System-defined permissions supported by HSS

Role/Policy Name	Description	Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS	System-defined role	<ul style="list-style-type: none">• It depends on the Tenant Guest role. Tenant Guest: A global role, which must be assigned in the global project.

Role/Policy Name	Description	Type	Dependency
HSS FullAccess	All HSS permissions	System-defined policy	None
HSS ReadOnlyAccess	Read-only permission for HSS	System-defined policy	None

Authorization Process

Figure 11-1 Process for granting permissions



1. Create a user group and assign permissions. On the IAM console, grant the **HSS Administrator** permission.
2. Create a user and add it to the group. On the IAM console, add the user to the group created in **1**.
3. Log in and verify permissions.
Log in to the HSS console as the created user, and verify that the user only has read permissions for HSS.
In **Service List** on the console, select any other services (for example, there is only the **HSS Administrator** policy). If a message indicating that the permission is insufficient is displayed, the **HSS Administrator** permission takes effect.

11.2 HSS Custom Policies

Custom policies can be created to supplement the system-defined policies of HSS.

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

- Visual editor: Select cloud services, actions, resources, and request conditions. You do not need to have knowledge of the policy syntax.
- JSON: Create a policy in JSON format or edit the JSON strings of an existing policy.

For details, see "Creating a Custom Policy" in *Identity and Access Management User Guide*. The following section contains examples of common HSS custom policies.

Example Custom Policies

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

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

- Example 2: Denying agent uninstallation

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

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

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

- Multi-action policies

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

```
{
  "Version": "1.1",
```

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

12 FAQs

12.1 About HSS

12.1.1 What Is HSS?

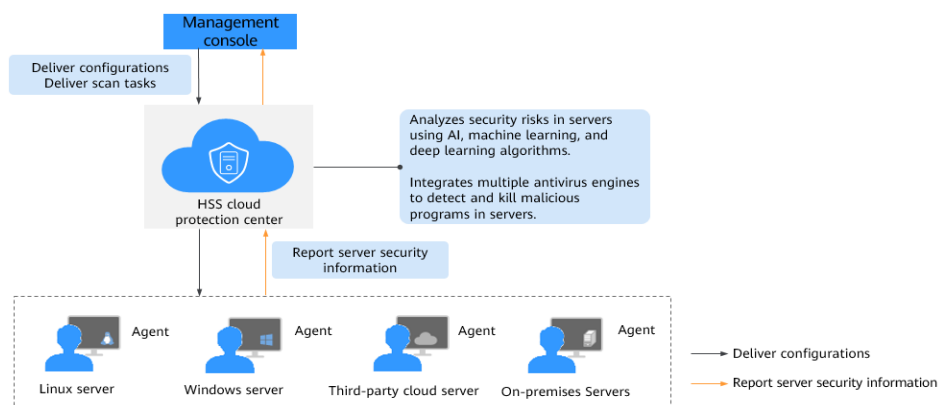
HSS helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats

How HSS Works

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 12-1 shows the working principle of HSS.

Figure 12-1 Working principles



The functions and working processes of HSS components are described as follows:

Table 12-1 Components

Component	Description
Management console	A visualized management platform, where you can apply configurations in a centralized manner and view the protection status and scan results of servers in a region.
HSS cloud protection center	<ul style="list-style-type: none">Analyzes security risks in servers using AI, machine learning, and deep learning algorithms.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	<ul style="list-style-type: none">Communicates with the HSS cloud protection center via HTTPS and WSS. Port 10190 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. <p>NOTE</p> <ul style="list-style-type: none">If no agent is installed or the agent installed is abnormal, the HSS is unavailable.Select the agent and installation command suitable for your OS.The HSS agent can be used for all editions, including container security and Web Tamper Protection (WTP). You only need to install the agent once on the same server.

12.1.2 What Is Container Security Service?

Container Security Service (CGS) scans vulnerabilities and configuration information in images, helping enterprises detect container risks that cannot be found using conventional security software. CGS also provides functions such as container process whitelist, container file monitoring, container information collection, and container escape detection to reduce risks.

12.1.3 What Is Web Tamper Protection?

Web Tamper Protection (WTP) monitors website directories in real time, backs up files, and restores tampered files using the backup. WTP protects your websites from Trojans, illegal links, and tampering.

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.

This section describes the operation process and main functions of WTP. See [Figure 12-2](#) and [Table 12-2](#).

Figure 12-2 WTP operation process

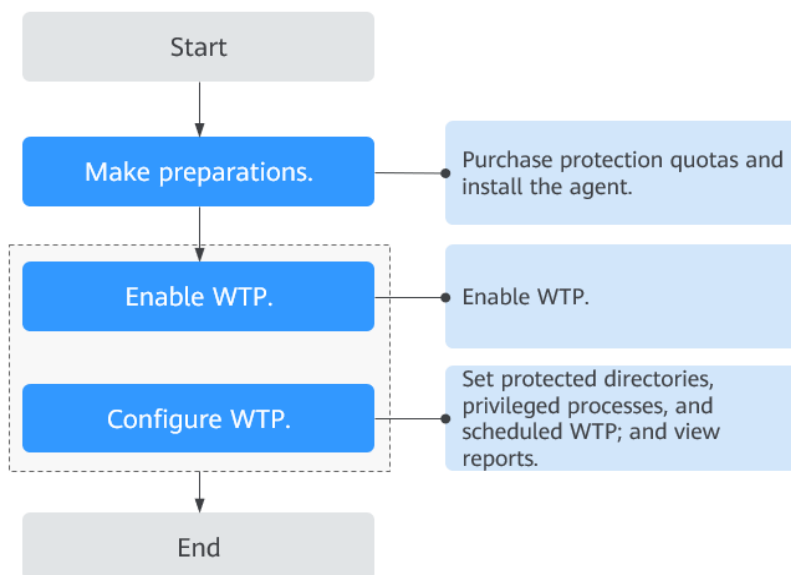


Table 12-2 WTP operation process and function description

Type	Operation	Description and Reference
Preparations	--	If no VDC operator account is available, contact an operations administrator to create a VDC administrator account, and then use the VDC administrator account to create a VDC operator.
Getting Started with WTP	Applying for Quota	Apply for WTP quota.
	Installing an Agent	The agent is provided by HSS. It runs scan tasks to scan all servers, monitors server security, and reports collected server information to the cloud protection center. You can enable WTP only after the agent is installed.
	Parameters required for configuring alarm notifications	After alarm notification is enabled, you can receive alarm notifications sent by HSS to learn about security risks facing your servers and web pages. Without this function, you have to log in to the management console to view alarms.

Type	Operation	Description and Reference
	Enabling HSS	Allocate a quota to a server and enable HSS for the server.
Enable WTP	Adding a Protected Directory	Add a directory to be protected by WTP.
	Create remote backup	By default, HSS backs up the files from the protected directories to the local backup directory you specified when you added protected directories. To protect the local backup files from tampering, you must enable the remote backup function.
	Adding a privileged process	After WTP is enabled, the content in the protected directories is read-only. To allow certain processes to modify files in the directories, add them to the privileged process list.
	Set scheduled WTP protection	You can schedule WTP protection to allow website updates in specific periods.
	Enabling dynamic WTP	Dynamic WTP protects your data while Tomcat is running, detecting dynamic data tampering in databases.
	View WTP reports	After WTP is enabled, HSS will immediately check the protected directories you specified. You can check records about detected tampering.

12.1.4 What Are the Relationships Between Images, Containers, and Applications?

- An image is a special file system. It provides programs, libraries, resources, configuration files and other files required for a running container. An image also contains some configuration parameters (such as anonymous volumes, environment variables, and users) prepared for a running container. An image does not contain any dynamic data, and its content is unchangeable after creation.
- The relationship between the image and container is similar to that between the class and instance in the program design. An image is static, and a container is the entity for a running image. A container can be created, started, stopped, deleted, and suspended.
- Multiple containers can be started for an image.
- An application may include one or a set of containers.

12.1.5 How Do I Use HSS?

To use the HSS, perform the following steps:

Step 1 .

Apply for protection quotas in the required edition.

Step 2 [Install the agent](#).

You can enable HSS after installing the agent.

Step 3 [Enable HSS](#).

- After the agent is installed, you can enable protection for the servers.
- Before enabling HSS, you need to allocate a quota to a specified server. If the service is disabled or the server is deleted, the quota can be allocated to other servers.

Step 4 [View detection results](#) and handle risks.

----End

12.1.6 Can HSS Protect Local IDC Servers?

Yes, as long as your servers connect to the Internet.

12.1.7 Is HSS in Conflict with Any Other Security Software?

HSS may conflict with DenyHosts, G01, or 360 Guard (server edition).

Conflicts Between the Agent and DenyHosts

For details, see [Is the Agent in Conflict with Any Other Security Software?](#)

Conflicts Between the Two-factor Authentication Function and G01 or 360 Guard (Server Edition)

On a Windows server where HSS is enabled, the two-factor authentication function may conflict with the login authentication function of G01 or 360 Guard (server edition). In this case, enable only one of the functions as needed.

12.1.8 What Are the Differences Between HSS and WAF?

HSS and Web Application Firewall (WAF) are provided by the cloud platform to help you defend servers, websites, and web applications against risks and threats, improving system security. It is recommended that the services be used together.

Table 12-3 Differences Between HSS and WAF

Service Name	Category	Protected Object	Function
HSS (HSS)	Infrastructure security	Servers	<ul style="list-style-type: none"> • Asset management • Vulnerability management • Intrusion detection • Baseline inspection • Web tamper protection
WAF	Application security	Web applications	<ul style="list-style-type: none"> • Basic web protection • CC attack protection • Precise protection

12.1.9 What Is the HSS Agent?

The HSS agent is used to scan all servers and containers, monitor their status in real time, and collect their information and report to the cloud protection center.

Functions of the Agent

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

 **NOTE**

- If no agent is installed or the agent installed is abnormal, the HSS is unavailable.

Linux Agent Processes

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

The agent contains the following processes:

Table 12-4 Linux agent processes

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

12.2 Agent FAQs

12.2.1 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.
- Procedure

- a. Log in as user **root** to ECS.
- b. 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
```

- c. Run the following command to stop DenyHosts:
- d. Run the following command to cancel the automatic start of DenyHosts upon host startup:

```
kill -9 'cat /var/lock/denyhosts'  
chkconfig --del denyhosts;
```

12.2.2 How Do I Install the Agent?

- For details about how to install the Linux agent, see [Installing an Agent on Linux](#).
- For details about how to install the Windows agent, see [Installing an Agent on Windows](#).

12.2.3 How Do I Uninstall the Agent?

Two uninstallation methods are available: one-click uninstallation and manual local uninstallation.

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.

- If the agent fails to be upgraded, uninstall the agent.

Prerequisites

When you uninstall the agent on the management console, the **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, click , select a region, and choose **Security > Host Security Service**.

Step 3 In the navigation pane, choose **Installation and Configuration**.

Step 4 On the displayed page, click the **Agents** tab and click **Online**. In the row containing the desired server, click **Uninstall Agent** in the **Operation** column.

Step 5 In the displayed dialog box, 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 agent on a server when you no longer use HSS or need to reinstall the agent.

NOTE

After the agent is uninstalled from the target 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 that you want to uninstall the 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**.

12.2.4 What Should I Do If Agent Installation Failed?

If this is the first time you install the agent, and the installation failed, rectify the fault by following the instructions provided in this section.

Symptoms

The agent fails to be installed by running commands. The server list page on the console still indicates that the agent is not installed.

Possible Causes

- The SELinux firewall has not been disabled.
- The root account is not used for installation.
- The installation command is incorrect.
- Residual information exists after the agent is uninstalled.

Solution

Step 1 Check whether the SELinux firewall of the server is disabled.

- If it is, go to the next step.
- If it is not, disable it and install the agent again.

Step 2 Check whether the installation command is suitable for the server region and OS.

1. Switch to the server region.
 2. Copy the installation commands suitable for your server OS.
 - Run 32-bit installation commands on a 32-bit server.
 - Run 64-bit installation commands on a 64-bit server.
- If yes, go to the next step.
 - If the commands you used are incorrect, install the agent again with correct ones.

Step 3 Check whether the installation was performed by user **root**.

- If yes, go to the next step.

- If it was not, install the agent again as user **root**.

Step 4 **Uninstall the agent** as user **root** and forcibly install it.

- If the installation is successful, no further action is required.
- If the installation fails, contact technical support.

----End

12.2.5 How Do I Fix an Abnormal Agent?

Your agent is probably abnormal if it is in **Not installed** or **Offline** state. Agent statuses and their meaning 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 agent status on the console is not updated.
The agent status has not been updated. After the agent is installed, it takes 5 to 10 minutes for the console to update its status.
- OS version not supported.
For details, see "Constraints" in "Service Overview".
- 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.

Solution

Step 1 Check whether the agent status remains **Offline** on the console for more than 10 minutes after the agent was installed.

- If yes, go to **2**.
- If no, wait until the agent goes online. No further action is required. After the agent was installed, it takes 5 to 10 minutes for the console to update its status.

Step 2 Check whether your server OS is within the scope of support in "Constraints" in "Service Overview".

- If yes, go to **3**.
- If no, the HSS agent cannot be installed or run on your server. Upgrade the OS to a version supported by HSS and try again.

Step 3 Check whether the server network is normal.

- If yes, go to **4**.
- If no, ensure the security group of your server allows access to port 10190 of the 100.125.0.0/16 CIDR block in the outbound direction and the server can

access the network. After the server can access the network, check the agent status.

Step 4 Restart the agent process.

- Windows
 - a. Log in to the server as user **administrator**.
 - b. Open the Task Manager.
 - c. On the **Services** tab page, select **HostGuard**.
 - d. Right-click the service and choose **Restart**.

- Linux

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

12.2.6 What Is the Default Agent Installation Path?

The agent installation paths on servers running the Linux or Windows OS cannot be customized. [Table 12-5](#) describes the default paths.

Table 12-5 Default agent installation paths

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

12.2.7 How Many CPU and Memory Resources Are Occupied by the Agent When It Performs Scans?

HSS uses lightweight agents, which occupy only a few resources and do not affect your services.

The CPU and memory usage is as follows.

Maximum CPU Usage

A running agent occupies a maximum of 20% of a vCPU. The actual usage depends on your server specifications. For details, see [Resource Usage of Different Specifications While the Agent Is Running](#).

If the CPU usage exceeds 20% of a vCPU, the agent will automatically reduce CPU usage, spending more time on scans. This does not affect your services. If the CPU usage exceeds 25% of a vCPU, the agent will be automatically restarted.

NOTE

The agent is scheduled to scan your servers from 00:00 to 04:00 every day, avoiding your service busy hours.

Peak Memory Usage

A running agent occupies about 500 MB memory.

If the memory usage reaches 500 MB, the agent will be automatically restarted within 5 minutes.

Resource Usage of Different Specifications While the Agent Is Running

The following table describes the CPU and memory usage of different specifications when the agent is running.

Table 12-6 Resource usage of the agent


vCPUs	Max. CPU Usage of Agent	Max. Memory Usage
1 vCPU	20%	500MB
2 vCPUs	10%	500MB
4 vCPUs	5%	500MB
8 vCPUs	2.5%	500MB
12 vCPUs	About 1.67%	500MB
16 vCPUs	About 1.25%	500MB
24 vCPUs	About 0.84%	500MB
32 vCPUs	About 0.63%	500MB
48 vCPUs	About 0.42%	500MB
60 vCPUs	About 0.34%	500MB
64 vCPUs	About 0.32%	500MB

12.2.8 Do WTP and HSS Use the Same Agent?

Yes.

All HSS editions can use the same agent installed on a server.

12.2.9 How Do I View 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, click , select a region, and choose **Security > Host Security Service**.
- Step 3** On the **Installation & Configuration** page, click the **Agents** tab and click **Offline**. View the servers where the agent is not 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.

Click **Offline Cause** to view the possible causes.

----End

12.3 Brute-force Attack Defense

12.3.1 How Does HSS Intercept Brute Force Attacks?

Types of Detectable Brute Force Attacks

HSS can detect the following types of brute force attacks:

- Windows: SqlServer (automatic interception is not supported currently) and Rdp
- Linux: MySQL, vfstp, and SSH

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 12-3 Added rules

```
root@qds2-349304-mysql03:/usr/local/hostguard/rog# iptables -nL
Chain INPUT (policy ACCEPT)
target prot opt source destination
IN_HIDS_MYSQLD_BIP_DROP tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306
IN_HIDS_MYSQLD_DENY_DROP tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Chain IN_HIDS_MYSQLD_BIP_DROP (1 references)
target prot opt source destination

Chain IN_HIDS_MYSQLD_DENY_DROP (1 references)
target prot opt source destination
```

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 Intercepted

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.**

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 blocked attacks on the **Intrusions** page of the HSS console.

Viewing Brute Force Cracking Detection Results

Step 1 Log in to the management console.

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

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

Step 4 Click **View Details** under **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

If you manually unblocked an IP address, but incorrect password attempts from this IP address reach the threshold again, this IP address will be blocked again.

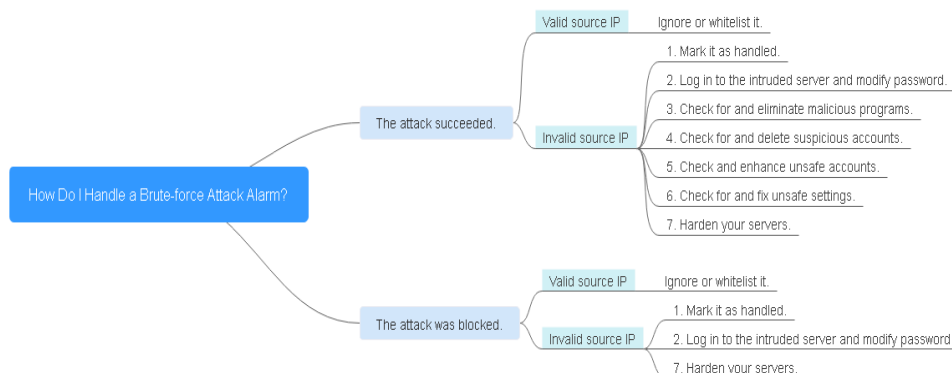
12.3.2 How Do I Handle a Brute-force Attack Alarm?

- If a brute-force attack succeeded, take immediate measures to prevent attackers from further actions, such as breaching data, performing DDoS attacks, or implanting ransomware, miners, or Trojans.
- If a brute-force attack was blocked, take immediate measures to enhance your servers.

Mind map for troubleshooting

The following mind map describes how to handle a brute-force attack alarm.


Figure 12-4 Mind map for troubleshooting



Handling the Alarm of a Successful Brute-force Attack

If you received an alarm notification indicating that your account had been cracked, you are advised to harden your servers as soon as possible.

Step 1 Log in to the management console.

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

Step 3 Check whether the IP address that triggered the alarm is valid.

Choose **Detection > Alarms**. In the **Event Types** area, choose **Abnormal User Behavior > Abnormal logins** and check the login IP address.

- If the IP address is from a normal user (for example, who entered incorrect password for multiple times but logged in before their account is blocked), your server is not intruded. In this case, you can click **Handle** and ignore the event.
- If the IP address is invalid, your server may have been intruded. In this case, mark this event as handled, log in to the intruded server, and change its password to a stronger one. For details, see [How Do I Set a Secure Password?](#)

Step 4 Check for and eliminate malicious programs.

Choose **Malware > Malicious programs** and check alarm events.

- If you find malicious programs implanted in your servers, locate them based on their process paths, users running them, and startup time. To kill a malicious program in an alarm event, click **Handle** in the row of this event and select **Isolate and kill**.
- If you have confirmed that all the malicious program alarms are false, go to [Step 8](#).

Step 5 Check for suspicious account change records.

Choose **Asset Management > Asset Fingerprints** and click the **Account Information** tab. Detect suspicious account change records to prevent attackers from creating accounts or escalating account permissions (for example, adding login permissions to an account). For details, see [Checking Operation History](#).

Step 6 Check and handle invalid accounts.

Choose **Detection > Alarms**. Choose **Abnormal User Behavior > Invalid accounts** to view and handle the invalid account alarms. For details, see [Handling Server Alarms](#).

Step 7 Check for and fix unsafe settings.

Check for and fix weak password complexity policies and unsafe software settings on your servers. For details, see [Suggestions on Fixing Unsafe Settings](#).

----End

Handling the Alarm of a Blocked Brute-force Attack

If you have enabled HSS, HSS will protect your servers against brute-force attacks.

You can configure a login security policy to specify the brute force cracking determination mode and blocking duration. For details, see [Login Security Check](#).

If you have not configured any login security detection policy, the following default login security policy is used: HSS will block an IP address if it has five or more brute-force attack attempts detected within 30 seconds, or 15 or more brute-force attack attempts detected within 3,600 seconds.


If you receive an alarm indicating that an attack source IP address is blocked, check whether the source IP address is a trusted IP address.

Constraints and Limitations

- Linux
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
 - 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.

Procedure

Step 1 Log in to the management console.

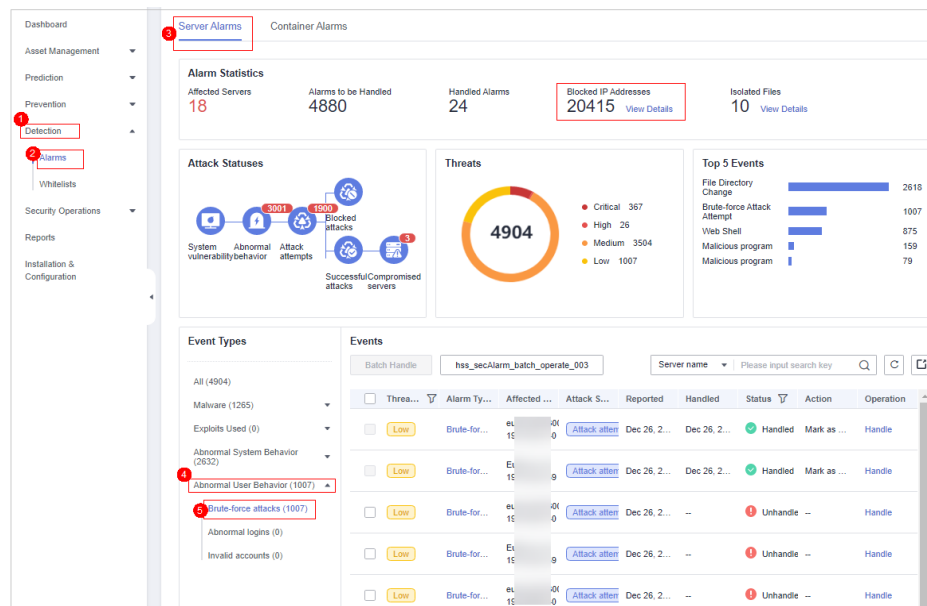
Step 2 In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.

Step 3 Choose **Detection > Alarms**. Choose **Abnormal User Behavior > Brute-force attacks** to view account brute force events.

Brute-force attack alarms will be generated if:

- The system uses weak passwords, is under brute-force attacks, and attacker IP addresses are blocked.
- Users fail to log in after several incorrect password attempts, and their IP addresses are blocked.

Figure 12-5 Brute-force attacks



Step 4 Check whether the login IP address triggering the alarm is valid.

- If the IP address is valid,
 - To handle a false alarm, click **Handle** in the row of the alarm event. Ignore or whitelist the IP address. This does not unblock the IP address.
 - To unblock the IP address, click **View Details** under **Blocked IP Addresses**, select the IP address, and unblock it. Alternatively, you can just wait for it to be automatically unblocked when its blocking duration expires. By default, suspicious SSH attackers are blocked for 12 hours. Other types of suspicious attackers are blocked for 24 hours.
- If the source IP address is invalid or unknown, Mark this event as handled. Immediately log in to your server and change your password to a stronger one.

----End

Helpful Links

- [How Does HSS Intercept Brute Force Attacks?](#)
- [How Do I Unblock an IP Address?](#)

12.3.3 How Do I Defend Against Brute-force Attacks?

Impact of Account Cracking

Intruders who cracked server accounts can exploit permissions to steal or tamper with data on servers, interrupting enterprise services and causing great loss.

Preventive Measures

- Configure the SSH login whitelist.
The SSH login whitelist allows logins from only whitelisted IP address, effectively preventing account cracking. For details, see [Configuring an SSH Login IP Address Whitelist](#).
- Enable 2FA.
2FA requires users to provide verification codes before they log in. The codes will be sent to their mobile phones or email boxes.
Choose **Installation & Configuration**. On the **Two-Factor Authentication** tab, select servers and click **Enable 2FA**. For details, see [Enabling 2FA](#).
- Use non-default ports.
Change the default remote management ports 22 and 3389 to other ports.
- Configure security group rules to prevent the attacking IP addresses from accessing your service ports.

NOTE

You are advised to allow only specified IP addresses to access open remote management ports (for example, for SSH and remote desktop login).

You can configure security group rules to control access to your servers. For a port used for remote login, you can set IP addresses that are allowed to remotely log in to your ECSs.

To allow IP address **192.168.20.2** to remotely access Linux ECSs in a security group over the SSH protocol and port 22, you can configure the following security group rule.

Table 12-7 Setting IP addresses to remotely connect to ECSs

Direction	Protocol/Application	Port	Source
Inbound	SSH (22)	22	For example, 192.168.20.2/32

- Set a strong password.
HSS baseline checks include the password policy check and weak password detection, which can find accounts that use weak passwords on your servers. You can view and handle password risks on the console.

12.3.4 How Do I Do If the Account Cracking Prevention Function Does Not Take Effect on Some Linux Accounts?

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 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)

12.3.5 How Do I Unblock an IP Address?

HSS will block an IP address if it has five or more brute-force attack attempts detected within 30 seconds, or 15 or more brute-force attack attempts detected within 3600 seconds. If a normal IP address is blocked by mistake (for example, after O&M personnel enter incorrect passwords for multiple times), you can unblock the IP address.


If you manually unblocked an IP address, but incorrect password attempts from this IP address reach the threshold again, this IP address will be blocked again.

 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.

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Detection > Alarms** and click **Server Alarms**.

Step 4 In the **Alarm Statistics** area, click **View Details** under **Blocked IP Addresses**.

Step 5 In the blocked IP address list, select an IP address and click **Cancel Interception**.

----End

12.3.6 What Do I Do If HSS Frequently Reports Brute-force Alarms?

An alarm indicates that an attack was detected. It does not mean your cloud servers have been intruded. If you receive an alarm, handle it and take countermeasures in a timely manner.

Possible Causes

No access control is configured for the ports used for remotely connecting to your servers. As a result, viruses on the network frequently attacked your ports.

Solution

Take any of the following measures.

- Configure the SSH login whitelist.
The SSH login whitelist allows logins from only whitelisted IP address, effectively preventing account cracking. For details, see [Configuring an SSH Login IP Address Whitelist](#).
- Enable 2FA.
2FA requires users to provide verification codes before they log in. The codes will be sent to their mobile phones or email boxes.
Choose **Installation & Configuration**. On the **Two-Factor Authentication** tab, select servers and click **Enable 2FA**. For details, see [Enabling 2FA](#).
- Use non-default ports.
Change the default remote management ports 22 and 3389 to other ports.
- Configure security group rules to prevent the attacking IP addresses from accessing your service ports.

NOTE

You are advised to allow only specified IP addresses to access open remote management ports (for example, for SSH and remote desktop login).

You can configure security group rules to control access to your servers. For a port used for remote login, you can set IP addresses that are allowed to remotely log in to your ECSs.

To allow IP address **192.168.20.2** to remotely access Linux ECSs in a security group over the SSH protocol and port 22, you can configure the following security group rule.

Table 12-8 Setting IP addresses to remotely connect to ECSs

Direction	Protocol/Application	Port	Source
Inbound	SSH (22)	22	For example, 192.168.20.2/32

- Set a strong password.

HSS baseline checks include the password policy check and weak password detection, which can find accounts that use weak passwords on your servers. You can view and handle password risks on the console.

How Does HSS Intercept Brute Force Attacks?

HSS can detect brute-force attacks on SSH, RDP, FTP, SQL Server, and MySQL accounts.

By default, HSS will block an IP address if it has five or more brute-force attack attempts detected within 30 seconds, or 15 or more brute-force attack attempts detected within 3600 seconds.

If you have enabled HSS, you can configure a login security policy to specify the brute force cracking determination mode and blocking duration. For details, see [Login Security Check](#).

To view the IP addresses blocked by HSS, choose **Detection** > **Alarms** and click the value above **Blocked IP Addresses**.

12.3.7 What Do I Do If My Remote Server Port Is Not Updated in Brute-force Attack Records?

Symptom

The remote port of a server has been changed, but the brute-force attack records still displays the old port.

Solution

The remote port configuration is synchronized to HSS through the agent. If the remote port is changed, perform the following operations to restart the agent:

- Windows: Log in to the server as an administrator. Open Task Manager, right-click **HostGuard** and choose **Restart** from the shortcut menu.
- Linux: Run the `service hostguard restart` command as user **root**.

12.4 Weak Passwords and Unsafe Accounts


12.4.1 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, click , select a region, and choose **Security > Host Security Service**.
- Step 3** Choose **Prediction > Baseline Checks** and click the **Common Weak Password Detection** tab.
- Step 4** Check the server, account name, account type, and usage duration of the weak password. Log in to the server and change the password.
- End

Changing a Weak Password

System	Procedure	Remarks
Windows OS	<p>To change the password in the Windows 10, perform the following steps:</p> <ol style="list-style-type: none"> 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	<p>Log in to the Linux server and run the following command:</p> <pre>passwd [<user>]</pre>	<p>If you do not specify any username, you are changing the password of the current user.</p> <p>After the command is executed, enter the new password as prompted.</p> <p>NOTE Replace <user> with the username.</p>

System	Procedure	Remarks
MySQL database	<ol style="list-style-type: none">Log in to the MySQL database.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;Run the following command to change the password: SET PASSWORD FOR 'Username'@'Host'=PASSWORD('New_password');Run the following command to refresh password settings: flush privileges;	None
Redis database	<ol style="list-style-type: none">Open the Redis database configuration file redis.conf.Run the following command to change the password: requirepass <password>;	<ul style="list-style-type: none">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. <p>NOTE Replace <i><password></i> with the new password.</p>
Tomcat	<ol style="list-style-type: none">Open the conf/tomcat-user.xml configuration file in the Tomcat root directory.Change the value of password under the user node to a strong password.	None

12.4.2 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
 - c. The password cannot be the username or the username in reverse order.
- 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
 - Phrases
 - 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.

12.4.3 Why Are the Weak Password Alarms Still Reported After the Weak Password Policy Is Disabled?

If you have enhanced passwords before disabling the weak password policy, the weak password alarm will not be reported again.

If you do not enhance passwords before disabling the weak password policy, the reported alarm will persist and be retained for 30 days.

- To enhance server security, you are advised to modify the accounts with weak passwords in a timely manner, such as SSH accounts.
- To protect internal data of your server, you are advised to modify software accounts that use weak passwords, such as MySQL accounts and FTP accounts.

After modifying weak passwords, you are advised to perform manual detection immediately to verify the result. If you do not perform manual verification and do

not disable the weak password scan, HSS will automatically check the settings the next day in the early morning.

12.5 Intrusions


12.5.1 What Do I Do If My Servers Are Subjected to a Mining Attack?

Take immediate measures to contain the attack, preventing miners from occupying CPU or affecting other applications. If a server is intruded by a mining program, the mining program may penetrate the intranet and persist on the intruded server.

You should also harden your servers to better block intrusions.

Troubleshooting Procedure

Step 1 Log in to the management console.

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

Step 3 Check **Abnormal process behavior** events.

Choose **Detection > Alarms** and click **Server Alarms**. Choose **Abnormal System Behavior > Abnormal process behavior** to view and handle the abnormal process behavior alarms. Click **Handle** in the **Operation** column of an event.

Step 4 Check auto-startup items. Some of your auto-startup items were probably created by attackers to start mining programs upon server restart.

Choose **Asset Management > Asset Fingerprints**, click **Auto-startup**, and select **Operation History** to view the change history.

----End

Hardening Servers

After you delete miner programs, harden your servers to better defend against intrusions.

Linux servers

1. Let HSS automatically scan your servers and applications in the early morning every day to help you detect and eliminate security risks.
2. Set stronger passwords for all accounts (including system and application accounts), or change the login mode to key-based login.
 - a. Set the security password. For details, see [How Do I Set a Secure Password?](#)
 - b. Use a key to log in to the server.
3. Strictly control the usage of system administrator accounts. Grant only the least permissions required for applications and middleware and strictly control their usage.

4. Configure access rules in security groups. Open only necessary ports. For special ports (such as remote login ports), only allow access from specified IP addresses or use VPN or bastion hosts to establish your own communications channels.

Windows servers

Use HSS to comprehensively check for and eliminate security risks. Improve your account, password, and authorization security.

- **Account hardening**

Account	Description	Procedure
Ensure default account security.	<ul style="list-style-type: none"> • Disable user Guest. • Disable and delete unnecessary accounts. (You are advised to disable inactive accounts for three months before deleting them.) 	<ol style="list-style-type: none"> 1. Open Control Panel. 2. Click Administrative Tools. Open Computer Management. 3. Choose System Tools > Local Users and Groups > Users. 4. Double-click Guest. In the Guest Properties window, select Account is disabled. 5. Click OK.
Assign accounts with only necessary permissions to users.	<p>Create users and user groups of specific types.</p> <p>Example: administrators, database users, audit users</p>	<ol style="list-style-type: none"> 1. Open Control Panel. 2. Click Administrative Tools. Open Computer Management. 3. Choose System Tools > Local Users and Groups. Create users and groups as needed.
Periodically check and delete unnecessary accounts.	Periodically delete or lock unnecessary accounts.	<ol style="list-style-type: none"> 1. Open Control Panel. 2. Click Administrative Tools. Open Computer Management. 3. Choose System Tools > Local Users and Groups. 4. Choose Users or User Groups and delete unnecessary users or user groups.
Do not display the last username.	Forbid the login page from displaying the latest logged in user.	<ol style="list-style-type: none"> 1. Open Control Panel. 2. Click Administrative Tools. Open Local Security Policy. 3. Choose Local Policies > Security Options. 4. Double-click Interactive logon: Do not display last user name. 5. In the displayed dialog box, select Enable and click OK.

- **Password hardening**

Setting	Description	Procedure
Complexity	In line with the requirements set in How Do I Set a Secure Password .	<ol style="list-style-type: none">1. Open Control Panel.2. Click Administrative Tools. Open Local Security Policy.3. Choose Account Policies > Password Policy.4. Enable the policy Password must meet complexity requirements.
Maximum password age	In static password authentication mode, force users to change their passwords every 90 days or at shorter intervals.	<ol style="list-style-type: none">1. Open Control Panel.2. Click Administrative Tools. Open Local Security Policy.3. Choose Account Policies > Password Policy.4. Set Maximum password age to 90 days or shorter.
Account lockout policy	In static password authentication mode, lock a user account if authentication for the user fails for 10 consecutive times.	<ol style="list-style-type: none">1. Open Control Panel.2. Click Administrative Tools. Open Local Security Policy.3. Choose Account Policies > Account Lockout Policy.4. Set Account lockout threshold to 10 or smaller.

- **Authorization hardening**

Authorization	Description	Procedure
Remote shutdowns	Assign the permission Force shutdown from a remote system only to the Administrators group.	<ol style="list-style-type: none">1. Open Control Panel.2. Click Administrative Tools. Open Local Security Policy.3. Choose Local Policies > User Rights Assignment.4. Assign the permission Force shutdown from a remote system only to the Administrators group.

Authoriza tion	Description	Procedure
Local shutdown	Assign the permission Shut down the system only to the Administrators group.	<ol style="list-style-type: none"> 1. Open Control Panel. 2. Click Administrative Tools. Open Local Security Policy. 3. Choose Local Policies > User Rights Assignment. 4. Assign the permission Shut down the system only to the Administrators group.
User rights assignmen t	Assign the permission Take ownership of files or other objects only to the Administrators group.	<ol style="list-style-type: none"> 1. Open Control Panel. 2. Click Administrative Tools. Open Local Security Policy. 3. Choose Local Policies > User Rights Assignment. 4. Assign the permission Shut down the system only to the Administrators group.
Login	Authorize users to log in to the computer locally.	<ol style="list-style-type: none"> 1. Open Control Panel. 2. Click Administrative Tools. Open Local Security Policy. 3. Choose Local Policies > User Rights Assignment. 4. Assign the permission Allow log on locally to the users you want to authorize.
Access from the network	Allow only the authorized users to access this computer from the network (for example, by network sharing). Access from other terminals are not allowed.	<ol style="list-style-type: none"> 1. Open Control Panel. 2. Click Administrative Tools. Open Local Security Policy. 3. Choose Local Policies > User Rights Assignment. 4. Assign the permission Access this computer from the network to the users you want to authorize.

12.5.2 Why a Process Is Still Isolated After It Was Whitelisted?

After you add a process to the whitelist, it will no longer trigger certain alarms, but its isolation will not be automatically canceled.

Isolating and Killing a Malicious Program

- Choose **Installation & Configuration** and click the **Security Configuration** tab. Click the **Isolation and Killing of Malicious Programs** tab and enable this function.

- Choose **Detection > Alarms**. In the **Events** area, manually isolate and kill malicious programs.

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.

Canceling the Isolation of Files

- Choose **Detection > Events**. In the **Alarm Statistics** area, click **View Details** under **Isolated Files**, and locate the target server and click **Restore** in the **Operation** column.

After you cancel isolation, the read/write permissions of files will be restored, but terminated processes will not be automatically started.

12.5.3 What Do I Do If a Mining Process Is Detected on a Server?

You are advised to:

1. Back up data and disable unnecessary ports.
2. Set a stronger server password.
3. Enable HSS. Your servers will be protected from mining processes by its intrusion detection functions, such as account cracking prevention, remote login detection, malicious program detection, and web shell detection; as well as malicious program killing and vulnerability fixing functions.

12.5.4 Why Some Attacks on Servers Are Not Detected?

- Intrusions to your servers before HSS is enabled cannot be detected.
- If you have applied for HSS, remember to enable it to detect intrusions.
- Web attacks cannot be detected, because HSS mainly defends your servers. To protect websites, you can consult the security Solution Architect or use other secure services (such as WAF and Anti-DDoS).

12.5.5 Can I Unblock an IP Address Blocked by HSS, and How?

Whether you can unblock an IP address depends on why it was blocked. An IP address will be blocked if it is regarded as the source of a brute-force attack, listed in the common IP blacklist, or not in the IP whitelist you set.

Checking for Account Cracking Attacks

- HSS blocks attacking IP addresses to prevent intrusions. 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.
- If you are sure that a source IP address can be trusted, you can manually unblock it. Choose **Detection > Alarms**, click **View Details** under **Blocked IP Addresses**, and unblock the IP address in the displayed slide-out panel.

If you manually unblocked an IP address, but incorrect password attempts from this IP address exceed the threshold again, this IP address will be blocked again.

IP Address in the Common IP Blacklist

You cannot manually unblock such IP addresses.

12.5.6 Why a Blocked IP Address Is Automatically Unblocked?

If a blocked IP address does not perform brute-force attacks in the next 24 hours, the IP address will be automatically unblocked.

12.5.7 How Often Does HSS Detect, Isolate, and Kill Malicious Programs?

Detection period: real-time detection

Isolation and killing period:

- If you have enabled automatic isolation and killing, the system will scan and kill viruses in real time.
- If you have not enabled automatic isolation and killing, you need to manually check and handle alarms.

NOTICE

1. HSS can detect, isolate and kill malicious programs (by cloud scan) and abnormal process behaviors. For more information, see [Editions](#).
 2. HSS isolation and killing can be automatically or manually performed.
 - For more information about automatic isolation and killing, see "Isolating and Killing Malicious Programs" in [Security Configuration](#).
 - For more information about manual isolation and killing, see "Isolating and Killing Files" in [Managing Isolated Files](#).
-

12.5.8 What Do I Do If an IP Address Is Blocked by HSS?

Check whether the blocked IP address is a malicious IP address or a normal one.

- If it is normal, [add it to the whitelist](#).
- If it is malicious, no further operations are required.

12.5.9 How Do I Defend Against Ransomware Attacks?

Generally, ransomware is spread through Trojan implantation, emails, files, vulnerabilities, bundles, and storage media.

To defend against ransomware intrusions, [prevent brute-force attacks](#) and handle HSS alarms in a timely manner.

12.6 Abnormal Logins

12.6.1 Why Do I Still Receive Remote Login Alarms After Configuring the Login IP Whitelist?

Even whitelisted IP addresses can certain trigger alarms. The SSH login IP address whitelist, login whitelist, and remote login functions focus on different aspects of security, as described in [Table 12-9](#).

Table 12-9 Functions

Function	Description	How to Mask Alarm
SSH login IP address whitelist	Only the IP addresses in this whitelist can log in to specified servers via SSH. NOTICE To avoid connection issues, ensure you have not missed necessary IP addresses before enabling this function.	-
Login whitelist	To reduce false brute-force attack alarms, add trusted login IP addresses and their destination server IP addresses to this whitelist.	Choose Detection > Whitelists . Click the Login Whitelist tab, and add IP addresses. HSS will not generate brute-force alarms for these IP addresses.
Remote login	Logins not from Common Login Locations and Common Login IP Addresses will trigger remote login alarms. You will be informed of new IP addresses that log in to your servers.	Choose Installation & Configuration and click Security Configuration . Add login information on the Common Login Locations and Common Login IP Addresses tabs. Whitelisted logins will no longer trigger remote alarms.


12.6.2 How Do I Check the User IP address of a Remote Login?

Alarm Policies

The remote login detection function checks for remote logins into your servers in real time. HSS generates an alarm if it detects logins from locations other than the common login locations you set.

Viewing Remote Login Records on the Console

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Detection > Alarms**, and click **Server Alarms**.

Step 4 In the **Event Type** area, Choose **Abnormal User Behavior > Abnormal logins**, and click **Remote Login**.

----End

Locally Viewing Remote Login Records

For Linux servers, you can view logs in `/var/log/secure` and `/var/log/message` directories, or run the `last` command to check whether there are abnormal login records.

12.6.3 How Do I Know Whether an Intrusion Succeeded?

- If you have enabled alarm notifications for intrusion detection, you will be notified immediately when an account is cracked or may be cracked.
- You can also check whether attack IP addresses are blocked on the **Detection** page.
- For more details, view logs in the `/var/log/secure` and `/var/log/message` on the Linux server, or run the `last` command to check for abnormal login records.

12.7 Unsafe Settings

12.7.1 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: the password must contain at least eight characters and must contain uppercase letters, lowercase letters, numbers, 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 12-10](#).

Example:

```
password requisite pam_cracklib.so try_first_pass retry=3 minlen=8  
dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 type=
```

NOTE

Set **dcredit**, **ucredit**, **lcredit**, and **ocredit** to negative numbers.

Table 12-10 Parameter description

Parameter	Description	Example
minlen	Minimum length of a password. For example, if you want the minimum length to be eight, set the minlen value to 8.	minlen=8
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

Parameter	Description	Example
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 12-10](#).
Example:
password requisite pam_cracklib.so retry=3 minlen=8 dcredit=-1
ucredit=-1 lcredit=-1 ocredit=-1 difok=3

12.7.2 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 the 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.

Step 2 Choose **Account Policies > Password Policy** and perform the following operations.


- 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.

Step 3 Run the **gpupdate** command to refresh your system settings. After the refresh succeeded, the settings will take effect in the system.

----End

12.7.3 How Do I Handle Unsafe Configurations?

HSS automatically performs a configuration detection for servers. You can repair unsafe configuration items or ignore the configuration items you trust based on the detection result.

- Modifying unsafe configuration items
View details about a detection rule, verify the detection result based on the audit description, and handle the exception based on the modification recommendation.
You are advised to repair the configurations with a high threat level immediately. The configurations with a medium or low threat level can be fixed later based on service requirements.
- Ignoring trusted configuration items
 - a. Click the name of an ECS to view its details. Choose **Baseline Checks > Unsafe Configurations**.
 - b. Locate the target risk item, click  in front of its name to expand the check items and click **Ignore** in the **Operation** column. You can also select multiple detection rules and click **Ignore** in the upper part of the page to ignore them in batches.
To unignore an ignored detection rule, click **Unignore** in the **Operation** column. You can also select multiple ignored detection rules and click **Unignore** in the upper part of the page to unignore them in batches.
- Verification
After modifying configuration items, you are advised to choose **Prediction > Vulnerabilities** and click **Scan** to perform manual scan immediately to verify the result.

12.7.4 How Do I View Configuration Check Reports?

You can view the configuration check details online.

Procedure

- Step 1** On the configuration check page, click a configuration check baseline name.
- Step 2** On the detection rule details page, click **View Details**.
- Step 3** You can rectify unsafe configuration items and ignore trusted configuration items based on the suggestions provided.

----End

12.8 Vulnerability Management

12.8.1 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 servers, Windows servers, 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.

----End

12.8.2 What Do I Do If an Alarm Still Exists After I Fixed a Vulnerability?

Perform the following operations to locate the cause and fix the problems.

NOTE

For more information, see the section "Fixing Vulnerabilities and Verifying the Result".

Possible Causes and Solutions on a Linux Server

- No yum sources have been configured.
In this case, configure a yum source suitable for your Linux OS, and fix the vulnerability again.
- The yum source does not have the latest upgrade package of the corresponding software.
Switch to the yum source having the required package and fix the vulnerability again.
- The intranet environment cannot connect to Internet.
Servers need to access the Internet and use external yum sources to fix vulnerabilities. If your servers cannot access the Internet, or the external image sources cannot provide stable services, you can use the image source.

- The old kernel version remains.
Old kernel versions often remain in servers after upgrade. You can run the [verification commands](#) to check whether the current kernel version meets the vulnerability fix requirements. If it does, ignore the vulnerability on the **Linux Vulnerabilities** tab of the **Vulnerabilities** page. You are not advised to delete the old kernel.

Table 12-11 Verification commands

OS	Verification Command
CentOS/Fedora /Euler/ Redhat/Oracle	<code>rpm -qa grep <i>Software_name</i></code>
Debian/Ubuntu	<code>dpkg -l grep <i>Software_name</i></code>
Gentoo	<code>emerge --search <i>Software_name</i></code>

- **The server is not restarted after the kernel vulnerability is fixed.**
After the kernel vulnerability is fixed, restart the server. If the server is not restarted, the vulnerability alarm still exists.

12.8.3 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.

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

After you fixed Windows OS vulnerabilities or Linux kernel vulnerabilities, you need to restart servers for the fix to take effect, or HSS will continue to warn you of these vulnerabilities. For other types of vulnerabilities, you do not need to restart servers after fixing them.

12.8.5 Can I Check the Vulnerability and Baseline Fix History on HSS?

Viewing Fixed Vulnerabilities

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Prediction > Vulnerabilities**.
- Step 4** On the vulnerability tabs, filter and view fixed vulnerabilities.


NOTICE

Vulnerabilities are displayed in the vulnerability list only for seven days. You can only check the vulnerabilities that have been fixed in the last seven days.

----End

Viewing Fixed Baseline Issues

The fix history does not show the password complexity policy settings or common weak passwords that have been fixed. To check other fixed configuration items, perform the following steps:

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Prediction > Baseline Checks**.
- Step 4** Click the **Unsafe Configurations** tab.
- Step 5** Click a baseline name to go to the details page.
- Step 6** On the **Check Items** tab, view the check items in **Passed** state.


----End

12.9 Web Tamper Protection

12.9.1 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.

12.9.2 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, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane, choose **Prevention > Web Tamper Protection**.
- Step 4** Locate the target server and click **Configure Protection** in the **Operation** column.
- Step 5** Click **Settings**. On the **Protected Directory Settings** page on the right, select the directory to be edited 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.

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

----End

12.9.3 What Should I Do If WTP Cannot Be Enabled?

The causes of this problem vary by scenarios.

Insufficient Quota

- **Symptom**
The WTP quota in the selected region is insufficient.

Agent Status Is Abnormal

- **Symptom**
The agent status is **Offline** or **Not installed** in the server list on the **Web Tamper Protection** page.
- **Solution**
Rectify the fault by following the instructions provided in [How Do I Fix an Abnormal Agent](#). Ensure that **Agent Status** in the server list is **Online**.

Enterprise Edition HSS Has Been Enabled

- **Symptom**
Protection Status is **Enabled** in the [server list](#) on the HSS console.
- **Solution**
Disable HSS and then [enable WTP](#).

 NOTE

HSS editions include the enterprise, premium, and WTP editions. Before enabling WTP for a server, ensure that enterprise and premium edition HSS has been disabled for the server.

Protection Was Enabled on the Wrong Page

To enable WTP, choose **Web Tamper Protection > Servers**.

 NOTE

If you have applied for the WTP edition, you can use all functions of the premium edition, and you can enable the server protection only on the **Web Tamper Protection**. After WTP is enabled, server protection of the premium edition is also enabled.

12.9.4 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.

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.

12.9.5 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.

12.9.6 What Are the Differences Between the Web Tamper Protection Functions of HSS and WAF?

The web tamper protection function of HSS monitors website directories in real time, backs up files, and restores tampered files using the backup, protecting websites from tampering. This function is helpful for governments, educational institutions, and enterprises.

WAF protects user data on the application layer. It supports cache configuration on static web pages. When a user accesses a web page, the system returns a cached page to the user and randomly checks whether the page has been tampered with.

Differences Between the Web Tamper Protection Functions of HSS and WAF

The following table describes the differences between HSS and WAF.

Table 12-12 Differences between the web tamper protection functions of HSS and WAF

Item	HSS	WAF
Static web page protection	<ul style="list-style-type: none"> • Drive file and web file locking Locks files in driver and web file directories to prevent attackers from tampering with them. • Privileged process management Allows privileged processes to modify web pages. 	<ul style="list-style-type: none"> • Static web pages can be cached on servers. • Privileged process management is not supported.
Dynamic web page protection	Protects your data while Tomcat is running, detecting dynamic data tampering in databases.	No
Backup and restoration	<ul style="list-style-type: none"> • Active backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local host to restore the file. • Remote backup and restoration 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. 	No
Suitable for	Websites that have high security requirements and difficult to be manually recovered	Websites that only require application-layer protection

Purchase Suggestion

Website	Service
Common websites	WAF web tamper protection + HSS enterprise edition
Websites that require strong protection and anti-tampering capabilities	WAF web tamper protection + HSS WTP

12.10 Container Guard Service


12.10.1 How Do I Disable Node Protection?

Before You Start

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Disable protection for one or multiple servers.

- **Disabling protection for a server**
 - a. In the node list, click **Disable Protection** in the **Operation** column of a server.
 - b. In the dialog box that is displayed, confirm the information and click **OK**.
 - c. Choose **Asset Management > Containers & Quota** and click the **Container Nodes** tab. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

 **CAUTION**

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

- **Disabling protection in batches**
 - a. In the node list, select servers, and click **Disable Protection** above the list.
 - b. In the dialog box that is displayed, confirm the information and click **OK**.
 - c. Choose **Asset Management > Containers & Quota** and click the **Container Nodes** tab. Check the protection status in the server list. If it is **Unprotected**, the protection has been disabled.

 **CAUTION**

Disabling protection does not affect services, but will increase security risks. You are advised to keep your servers protected.

----End

12.10.2 What Is the Log Processing Mechanism of CGS?


CGS updates logs in its log file every 10 minutes. If the file exceeds 30 MB, CGS will back up the latest 30 MB logs to a backup file and clear the content of the log file.

The name of the backup log file is the name of the log file plus the extension **.last**. For example, the backup file of **shield.log** is **shield.log.last**.

12.10.3 How Do I Enable Node Protection?

When you enable node protection, the system automatically installs the CGS plugin on the node.

Step 1 Log in to the management console.

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

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

Step 4 In the **Operation** column of a node, click **Enable Protection**.

Step 5 Click **OK** to enable protection for the node. If **Protection Status** of the node is **Protected**, protection is enabled for the node.

 **NOTE**

- An HSS quota protects one cluster node.

----End

12.10.4 How Do I Enable the API Server Audit for an On-Premises Kubernetes Container?

Scenario

On-premises Kubernetes containers are used.

Prerequisites

- Container protection has been enabled.
- API server audit is disabled. Perform the following steps to check its status:
 - a. Log in to the node where kube-apiserver is located.
 - b. Check the **kube-apiserver.yaml** file or the started kube-apiserver process.
 - Go to the **/etc/kubernetes/manifest** directory and check whether **--audit-log-path** and **--audit-policy-file** exist in **kube-apiserver.yaml**. If they do not exist, API server audit is disabled.
 - Run the **ps** command to check whether **--audit-log-path** and **--audit-policy-file** exist in the command lines of the kube-apiserver process. If they do not exist, the audit function of the kube-apiserver process is disabled.

Enabling API Server Audit

Step 1 Copy the following YAML content and save it to a TXT file:

This YAML file is the configuration file of the Kubernetes audit function. You can directly use the file or compile it as needed.

```
apiVersion: audit.k8s.io/v1 # This is required.
kind: Policy
# Don't generate audit events for all requests in RequestReceived stage.
omitStages:
  - "RequestReceived"
rules:
  # The following requests were manually identified as high-volume and low-risk,
  # so drop them.
  # Kube-Proxy running on each node will watch services and endpoint objects in real time
  - level: None
    users: ["system:kube-proxy"]
    verbs: ["watch"]
    resources:
      - group: "" # core
        resources: ["endpoints", "services"]
  # Some health checks
  - level: None
    users: ["kubelet"] # legacy kubelet identity
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes"]
  - level: None
    userGroups: ["system:nodes"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes"]
  - level: None
    users: ["system:apiserver"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["namespaces"]
  # Some system component certificates reuse the master user, which cannot be accurately distinguished
  # from user behavior,
  # considering that subsequent new functions may continue to add system operations under kube-system,
  # the cost of targeted configuration is relatively high,
  # in terms of the overall strategy, it is not recommended (allowed) for users to operate under the kube-
  # system,
  # so overall drop has no direct impact on user experience
  - level: None
    verbs: ["get", "update"]
    namespaces: ["kube-system"]
  # Don't log these read-only URLs.
  - level: None
    nonResourceURLs:
      - /healthz*
      - /version
      - /swagger*
  # Don't log events requests.
  - level: None
    resources:
      - group: "" # core
        resources: ["events"]
  # Don't log leases requests
  - level: None
    verbs: [ "get", "update" ]
    resources:
      - group: "coordination.k8s.io"
        resources: ["leases"]
  # Secrets, ConfigMaps, and TokenReviews can contain sensitive & binary data,
  # so only log at the Metadata level.
```

```
- level: Metadata
resources:
  - group: "" # core
    resources: ["secrets", "configmaps"]
  - group: authentication.k8s.io
    resources: ["tokenreviews"]
# Get responses can be large; skip them.
- level: Request
verbs: ["get", "list", "watch"]
resources:
  - group: "" # core
  - group: "admissionregistration.k8s.io"
  - group: "apps"
  - group: "authentication.k8s.io"
  - group: "authorization.k8s.io"
  - group: "autoscaling"
  - group: "batch"
  - group: "certificates.k8s.io"
  - group: "extensions"
  - group: "networking.k8s.io"
  - group: "policy"
  - group: "rbac.authorization.k8s.io"
  - group: "settings.k8s.io"
  - group: "storage.k8s.io"
# Default level for known APIs
- level: RequestResponse
resources:
  - group: "" # core
  - group: "admissionregistration.k8s.io"
  - group: "apps"
  - group: "authentication.k8s.io"
  - group: "authorization.k8s.io"
  - group: "autoscaling"
  - group: "batch"
  - group: "certificates.k8s.io"
  - group: "extensions"
  - group: "networking.k8s.io"
  - group: "policy"
  - group: "rbac.authorization.k8s.io"
  - group: "settings.k8s.io"
  - group: "storage.k8s.io"
# Default level for all other requests.
- level: Metadata
```

Step 2 Upload the TXT file to the node where kube-apiserver is deployed.

Step 3 Go to the `/etc/kubernetes/manifest` directory and add the following content to the `kube-apiserver.yaml` file to enable API server audit:

```
--audit-policy-file=/etc/kubernetes/audit-policy.yaml \
--audit-log-path=/var/log/kubernetes/audit/audit.log \
--audit-log-maxsize=100 \
--audit-log-maxage=1 \
--audit-log-maxbackup=10
```

NOTE

--audit-policy-file: configuration file used by the audit function.

--audit-log-path: path of the log file where audit events are written. If this flag is not specified, the logging backend will be disabled.

--audit-log-maxsize: maximum size (in MB) of an audit log file before rotation.

--audit-log-maxage: maximum number of days for storing old audit log files.

--audit-log-maxbackup: maximum number of retained audit log files.

Step 4 (Optional) If your kube-apiserver runs as a pod, perform the following steps to persist logs on the server:

1. Locate the **volumeMounts** field in **kube-apiserver.yaml** and configure volume mounting as follows:

```
volumeMounts:  
- mountPath: /etc/kubernetes/audit-policy.yaml  
  name: audit  
  readOnly: true  
- mountPath: /var/log/kubernetes/audit/  
  name: audit-log  
  readOnly: false
```

2. Locate the **volumes** field in **kube-apiserver.yaml** and configure it as follows:

```
volumes:  
- name: audit  
  hostPath:  
    path: /etc/kubernetes/audit-policy.yaml  
    type: File  
- name: audit-log  
  hostPath:  
    path: /var/log/kubernetes/audit/  
    type: DirectoryOrCreate
```

----End

12.11 Ransomware Protection

12.11.1 What Are the Differences Between Ransomware Protection Backup and Cloud Backup?

The backup of HSS ransomware protection depends on Cloud Backup and Recovery (CBR). The server backup policy takes effect only after CBR is purchased.

There is no difference between the two in terms of backup mechanism and management. The only difference is that ransomware backup generates a dedicated ransomware backup library.

The backup mechanism of ransomware protection inherits that of CBR (Cloud Backup and Restoration). Backup files of ransomware protection can be centrally managed and viewed in CBR.


12.12 Security Configurations

12.12.1 How Do I Clear the SSH Login IP Address Whitelist Configured in HSS?

You can disable or delete the SSH login IP address whitelist.

Procedure

Step 1 Log in to the management console.

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

Step 3 Choose **Installation and Configuration**, click **Security Configuration**, and click **SSH IP Whitelist**.

- Step 4** Locate the row that contains the target whitelisted IP address and click **Disable** or **Delete** in the **Operation** column.

----End

12.12.2 What Can I Do If I Cannot Remotely Log In to a Server via SSH?

Symptoms

You can log in to a server via the console but not via SSH.

Possible Causes

- A server will be blocked if it is regarded as a suspicious server performing brute-force attacks (for example, the number of incorrect password attempts reaches 5 within 30 seconds).
- The SSH login IP whitelist is enabled. Your login IP addresses have not been added to the login whitelist.

If you enable the SSH login IP address whitelist, SSH logins will be allowed only from whitelisted IP addresses.

Solution

- Step 1** Check whether your login IP address was blocked because it was regarded as a source of brute-force attacks.

- If your login IP address was blocked as an attack source, go to the **Events** page, click **Blocked IP Addresses**, and unblock your IP address.
- If your login IP address was not blocked for this reason, go to [Step 2](#).

- Step 2** Check whether your login IP address is blocked because it is not whitelisted and the SSH login IP whitelist is enabled.

- If your login IP address was not blocked for this reason, add the IP address to the [SSH login IP address whitelist](#).
- If your login IP address was not blocked for this reason, contact technical support.

----End

12.12.3 How Do I Use 2FA?

This FAQ shows you how to use 2FA.

Enabling 2FA

For details, see [Enabling Two-factor Authentication](#).

Logging In and Passing 2FA Authentication


- Logging in to a Linux server
 - a. Use PuTTY or Xshell to log in to your server.

Select **Keyboard Interactive** and enter the user identity information.

- PuTTY
Set the authentication mode to **Keyboard Interactive** and click **OK**.
 - Xshell
In the **New Session Properties** dialog box, choose **Connection > Authentication > Method**, choose **Keyboard Interactive** from the **Method** drop-down list, and click **OK**.
- b. Enter the account and password of the server.
 - c. Enter the 2FA verification code sent to your terminal.

Figure 12-6 Entering a verification code

```
[root@PEK1000164604 /]# ssh 10.154.73.252
Authorized users only. All activities may be monitored and reported.
Password:
Input #25 Code:
```

- Logging in to a Windows server
 - a. Click **Start**, enter **Remote Desktop Connection** in the search box, and press **Enter** to open the remote desktop connection.
 - b. Enter the IP address of the host in the **Computer** text box and click **Connect**.
 - c. Enter the reserved mobile number or email address to receive 2FA verification code.
 - d. Enter the verification code, server account name, and password on the login page, and click  to log in to the server.

12.12.4 What Do I Do If I Cannot Enable 2FA?

Symptoms

- In the 2FA list, there are no servers with disabled 2FA.
- After 2FA is enabled, it does not take effect.
- Failed to enable 2FA.

Possible Causes

- Server protection is not enabled.
- 2FA settings have not taken effect. After 2FA is enabled, it takes about 5 minutes for the settings to take effect.
- For a Linux server, **Key pair** is selected as the login mode.
- The SELinux firewall is not disabled.

Solution

- Step 1** Check whether HSS has been enabled for the server for which you want to use 2FA.

- If it has, go to [Step 2](#).
- If it has not, enable HSS first.

Step 2 Check whether it has been 5 minutes since you enabled 2FA.

- If it has, go to [Step 3](#).
- If it has not, wait for 5 minutes and check whether 2FA takes effect.

Step 3 Check whether your server is a Linux server with **Key pair** selected as its login mode.

- If it is, disable the **Key pair** login mode and enable the **Password** login mode.
- If it is not, go to [4](#).

Step 4 Check whether the SELinux firewall is disabled on your server.

- If it is, go to [Step 5](#).
- If it is not, run either of the following commands to disable it.
 - To temporarily disable the SELinux firewall, run the following command:
setenfore 0 #Temporarily disable
 - To permanently disable the SELinux firewall, run the following command:
vi /etc/selinux config
selinux=disabled #Permanently disable

Step 5 Contact technical support.

----End

12.12.5 Why Can't I Receive a Verification Code After 2FA Is Enabled?

- The two-factor authentication function does not take effect immediately after being enabled.

Wait for 5 minutes and try again.

- To enable two-factor authentication, you need to disable the SELinux firewall. [Disable the SELinux firewall](#) and try again.
- Linux servers require user passwords for login.

To switch from the key login mode to password login mode, perform the following steps:

- a. Use the key to log in to the Linux ECS and set the password of user **root**.
sudo passwd root

If the key file is lost or damaged, reset the password of user **root**.

- b. Modify the SSH configuration file on the ECS as user **root**.

su root

vi /etc/ssh/sshd_config

Modify the following settings:

- Change **PasswordAuthentication no** to **PasswordAuthentication yes**.

Alternatively, delete the comment tag (#) before **PasswordAuthentication yes**.

- Change **PermitRootLogin no** to **PermitRootLogin yes**.
Alternatively, delete the comment tag (#) before **PermitRootLogin yes**.
- c. Restart sshd for the modification to take effect.
service sshd restart
- d. Restart the ECS. Then, you can log in to the ECS as user **root** using the password.

 NOTE

To prevent unauthorized users from using the key file to access the Linux ECS, delete the `/root/.ssh/authorized_keys` file or clear the `authorized_keys` file.

12.12.6 Why Does My Login Fail After I Enable 2FA?

The login failed probably because file configurations or the login mode was incorrect.

Correcting File Configurations

Check whether the configuration file is correct.

Configuration file path: `/etc/ssh/sshd_config`

Configuration items:

`PermitEmptyPasswords no`

`UsePAM yes`

`ChallengeResponseAuthentication yes`

NOTICE

If you use the **root** account for login, the following configuration item is required:
`PermitRootLogin yes`

Correcting the Login Mode

If you attempted to log in in either of the following ways, your login would fail.

- Used CloudShell to log in to an ECS.
- Attempted to log in to a Linux server through a CBH instance.

Failure cause: 2FA is implemented through a built-in module, which cannot be displayed if you log in in the preceding ways. As a result, the login authentication fails.

Solution: Perform login authentication by referring to [How Do I Use 2FA?](#)

12.12.7 How Do I Add a Mobile Phone Number or Email Address for Receiving 2FA Verification Notifications?

You can set your mobile phone number only if you have selected **SMS/Email** for **Method**. Set your mobile phone number in the SMN topic you choose.

In the **SMN Topic** drop-down list, only the SMN topics with confirmed subscriptions are displayed.

- You can click **View** to go to the SMN console and create a topic. Click **Add Subscription** and enter a mobile phone number or email address.
- You can also add or modify the mobile phone number or email address under an existing topic.
 - Adding a mobile phone number or email address
Click **View Topics**. Click **Add Subscription** and enter a mobile phone number or email address.
 - Deleting a mobile phone number or email address
Click **View Topics**. Click a topic name to go to the details page. Click the **Subscriptions** tab and delete one or more target endpoints.

12.12.8 If I Choose to Use Verification Code for 2FA, How Do I Get the Code?

If you want to enable 2FA but cannot receive messages through mobile phone or email, you can set **Method** to **Verification code**. Every time you log in to an ECS, HSS will send a random verification code to your login page. You simply need to enter the code to log in.

12.12.9 How Do I Disable the SELinux Firewall?

Security-Enhanced Linux (SELinux) is a kernel module and security subsystem of Linux.

SELinux minimizes the resources that can be accessed by service processes in the system (the principle of least privilege).

Closure Description

- After the SELinux is disabled, services are not affected.
- SELinux can be disabled temporarily or permanently as required.

Scenario

To use the two-factor authentication function of HSS, you need to permanently disable the SELinux firewall.

Procedure

Step 1 Remotely log in to the destination server.

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 PuTTY or Xshell, to log in to the server and install the agent on the server as user **root**.

Step 2 Run the shutdown command in the command window.

- **Temporarily disable SELinux**

Run the following command in the CLI to temporarily disable SELinux:

```
setenforce 0
```

 **NOTE**

After the system is restarted, the SELinux will be enabled again.

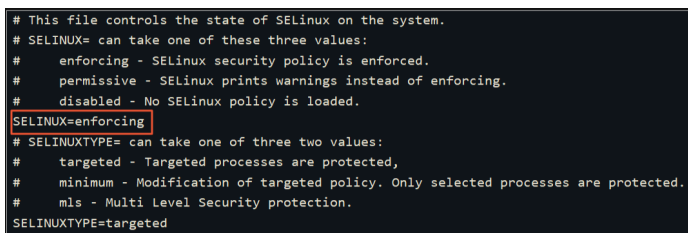
- **Permanently disable SELinux**

a. Run the following command in the directory window to edit the **config** file of SELinux:

```
vi /etc/selinux/config
```

b. Locate **SELINUX=enforcing**, press **i** to enter the editing mode, and change the parameter to **SELINUX=disabled**.

Figure 12-7 Editing the SELinux status



```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of three two values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

c. After the modification, press **Esc** and run the following command to save the file and exit:

```
:wq
```

Step 3 Run the permanent shutdown command, save the settings, and exit. Run the following command to restart the server immediately:

```
shutdown -r now
```

 **NOTE**

The permanent shutdown command takes effect only after the server is restarted.

Step 4 After the restart, run the following command to verify that SELinux is disabled:


```
getenforce
```

----End

12.13 Quotas

12.13.1 How Do I Filter Unprotected Servers?

Step 1 Log in to the management console.

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

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

Step 4 On the **Servers** tab, filter unprotected servers.

Step 5 Check the unprotected servers.

----End

12.13.2 What Do I Do If My Quotas Are Insufficient and I Failed to Enable Protection?

No Quotas

If you do not have sufficient quotas, quotas in the region where your servers are deployed. For details, see .

Checking Your Page

- To enable the enterprise or premium edition HSS, choose **Host Security Service > Servers**, and enable it on the **Servers** tab.
- If you have applied for the WTP edition, on the HSS console, choose **Prevention > Web Tamper Protection** and click the **Server** tab.
- If you have applied for the container edition, on the HSS console, choose **Containers & Quota** and click the **Servers** tab.

12.13.3 If I Change the OS of a Protected Server, Does It Affect My HSS Quota?

No. But before changing the server OS, you need to check whether the HSS agent supports the new OS. To obtain better HSS service experience, you are advised to install or upgrade to an OS version supported by the agent.

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

NOTICE

The agent is probably incompatible with the Linux or Windows 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 12-13 Server OSs supported by the agent

OS Type	System Architecture	Supported OS
Windows	X86	<ul style="list-style-type: none"> • Windows Server 2019 Datacenter 64-bit English (40 GB) • Windows Server 2019 Datacenter 64-bit Chinese (40 GB) • Windows Server 2016 Standard 64-bit English (40 GB) • Windows Server 2016 Standard 64-bit Chinese (40 GB) • Windows Server 2016 Datacenter 64-bit English (40 GB) • Windows Server 2016 Datacenter 64-bit Chinese (40 GB) • Windows Server 2012 R2 Standard 64-bit English (40 GB) • Windows Server 2012 R2 Standard 64-bit Chinese (40 GB) • Windows Server 2012 R2 Datacenter 64-bit English (40 GB) • Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB) <p>NOTE 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.</p>
Linux	X86	<ul style="list-style-type: none"> • CentOS 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8, 9 (64-bit) • Debian 9, 10, 11.0.0, 11.1.0 (64-bit) • EulerOS 2.2, 2.3, 2.5, 2.7 and 2.9 (64-bit) • Fedora 28 (64-bit) • Ubuntu 16, 18, 20.03, 20.04, 22.04 (64-bit) • Red Hat 7.4, 7.6, 8.0, 8.7 (64-bit) • OpenEuler 20.03 LTS, 22.03 SP3 LTS, 22.03 (64-bit) • AlmaLinux 9.0 (64-bit) • Rocky Linux 8.4, 8.5 and 9.0 (64-bit) • HCE 2.0 (64-bit) • Suse 12 SP5, 15 SP2, 15.5 (64-bit)
	ARM	<ul style="list-style-type: none"> • CentOS 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, and 9 (64-bit) • EulerOS 2.8 and 2.9 (64-bit) • Fedora 29 (64-bit) • Ubuntu 18 (64-bit) • Kylin V7 and V10 (64-bit) • HCE 2.0 (64-bit) • UOS V20 (64-bit)

12.14 Others

12.14.1 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**.
- 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**.
- Step 4** In the displayed dialog box, enter the user password of the server and click **OK** to connect to the server.

----End

12.14.2 How Do I Check HSS Log Files?

Log Path

The following table describes log files and their paths.

OS	Log Directory	Log File
Linux	/var/log/hostguard/	<ul style="list-style-type: none"> • hostwatch.log • hostguard.log • upgrade.log • hostguard-service.log • config_tool.log • engine.log
Windows	C:\Program Files\HostGuard \log	<ul style="list-style-type: none"> • hostwatch.log • hostguard.log • upgrade.log

Log Retention

Log File	Description	Maximum Size	Retained File	Retention Period
hostwatch.log	Records logs generated during the running of daemon processes.	10M	Latest eight files	Until the HSS agent is uninstalled
hostguard.log	Records logs generated during the running of working processes.	10M	Latest eight files	
upgrade.log	Records logs generated during version upgrading.	10M	Latest eight files	
hostguard-service.log	Records logs (scripts) generated when the service starts.	100k	Latest two logs	
config_tool.log	Records logs (programs) generated when the service starts.	10M	Latest two logs	
engine.log	Records logs generated when the service exits.	10M	Latest two logs	

12.14.3 How Do I Enable Logging for Login Failures?

MySQL

The account hacking prevention function for Linux 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 Linux OS, modify the **my.conf** file by adding **log_warnings=2** to **[MySQLd]**.
----End

vsftpd

This section shows you how to enable logging for vsftpd 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 vsftpd service. If the setting is successful, log records shown in the logs shown in [Figure 12-8](#) will be returned when you log in to vsftpd.

Figure 12-8 Log Records

```
Wed Aug 29 14:53:05 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"  
Wed Aug 29 14:53:11 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"  
Wed Aug 29 14:55:14 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"  
Wed Aug 29 14:55:18 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"  
Wed Aug 29 14:55:26 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"  
Wed Sep 5 11:50:16 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"  
Wed Sep 5 11:50:23 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"  
Wed Sep 5 13:59:53 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"  
Wed Sep 5 13:59:59 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"  
Wed Sep 5 14:00:08 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"
```

----End

12.14.4 How Do I Clear an Alarm on Critical File Changes?

If you are sure the changes on your critical files are safe, you do not need to handle the alarm. It will be automatically cleared in seven days.

12.14.5 Is HSS Available as Offline Software?

No.

12.14.6 How Do I Enable HSS Self-Protection?

HSS self-protection protect HSS files, processes, and software from malicious programs, which may uninstall HSS agents, tamper with HSS files, or stop HSS processes.


Constraints

- HSS self-protection is supported only for Windows servers that enabled HSS premium or WTP edition.
- Self-protection depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled. For more details, see:
 - [Enabling Ransomware Prevention](#)
 - Antivirus detection and HIPS detection are enabled by default. If you manually disable the two detection items, enable them again by referring to [Viewing a Policy Group](#).
- Enabling the self-protection policy has the following impacts:
 - The HSS agent cannot be uninstalled on the control panel of a server, but can be uninstalled on the HSS console.

- HSS process cannot be terminated.
- In the agent installation path **C:\Program Files\HostGuard**, you can only access the **log** and **data** directories (and the **upgrade** directory, if your agent has been upgraded).

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Security Operations > Policies**

Step 4 Click the name of a premium edition policy group for Windows servers. The policy group details page is displayed.

Select the policy group of the server where you want to enable self-protection.

- If you have not created any policy groups of premium edition, select the default policy group **tenant_windows_premium_default_policy_group**.
- If you have created policy groups of premium edition, select the policy group of your server. Perform the following operations:
 - a. In the navigation tree on the left, choose **Asset Management > Servers & Quota**.
 - b. Click the **Servers** tab to view the policy groups of servers.

Step 5 In the row containing the target self-protection policy, click **Enable** in the **Operation** column.

Step 6 In the displayed Prompt dialog box, click **OK**.

----End

Related Operations

Disabling HSS Self-Protection

Step 1 In the row containing the target self-protection policy, click **Disable** in the **Operation** column.

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




----End

12.14.7 What Do I Do If HSS Self-Protection Cannot Be Disabled?

Root Causes

If the server network is disconnected, agents cannot receive the command for disabling self-protection delivered by the HSS console. Therefore, HSS self-protection cannot be disabled.

Solutions

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the page, click , select a region, and choose **Security > Host Security Service**.
- Step 3** In the navigation pane on the left, choose **Asset Management > Servers & Quota**.
- Step 4** Click the **Servers** tab, click  in the upper right corner of the server list and select **Agent ID**.
- Step 5** Above the server list, enter a server name or ID and click  to search for the Windows server for which you want to disable the HSS self-protection.
- Step 6** In the row of the target Windows server, copy the first eight characters from the **Agent ID** column.
- Step 7** Open the CLI of the target Windows server.
- Step 8** Run the following command to disable HSS self-protection:

```
"C:\Program Files\HostGuard\bin\HssClient.exe"1234abcd
```

NOTE

1234abcd in the command indicates the first eight characters of the agent ID. The first eight characters of the agent ID are used as the verification code when **HSSClient.exe** is executed. It is to prevent malicious programs from disabling self-protection and user misoperations. Self-protection can be disabled only when the first eight characters of the agent ID are correct.

- Step 9** If **Disable self protect succeed.** is displayed, HSS self-protection is disabled successfully.

----End

A Change History

Released On	Description
2024-04-15	This issue is the first official release.